IBM Tivoli Directory Server

Installation and Configuration Guide

Version 5.2

SC32-1338-00

IBM Tivoli Directory Server

Installation and Configuration Guide

Version 5.2

SC32-1338-00

Note

Before using this information and the product it supports, read the general information under Appendix L, “Notices”, on page 191.

First Edition (October 2003)

This edition applies to version 5, release 2, of IBM Tivoli Directory Server and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1998, 2003. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface vii
Who should read this book vii
Publications vii
  IBM Tivoli Directory Server library vii
  Related publications viii
  Accessing publications online viii
Accessibility viii
Contacting software support viii
Conventions used in this book ix
  Typeface conventions ix
  Operating system differences. ix

Chapter 1. Quick installation path. . . . 1

Chapter 2. About this release 3
What's new for this release 3
Support for industry standards 7

Chapter 3. Installation, configuration, and migration overview 9
Migration from a previous release 9
Before you install: zip, tar, and iso files 9
Installation 10
Configuration 10

Chapter 4. System requirements. . . . 13
Requirements for the client 13
  Windows operating systems client requirements 13
  AIX operating system client requirements . . . 13
  xSeries Linux operating system client requirements 14
  zSeries Linux operating system client requirements 15
  iSeries and pSeries Linux operating system client requirements 16
  Solaris operating system client requirements . . 16
  Hewlett-Packard UNIX (HP-UX) operating system client requirements 17
Requirements for the server (including the client) . 18
  Windows operating systems server requirements 18
  AIX operating system server requirements . . . 19
  xSeries Linux operating system server requirements 20
  zSeries Linux operating system server requirements 22
  iSeries and pSeries Linux operating system server requirements 23
  Solaris operating system server requirements . . 24
  HP-UX operating system server requirements . . 25
Requirements for the Web Administration Tool . . 26
Secure Sockets Layer (SSL) Global Security Kit (GSKit) 28

Chapter 5. Migration from previous releases 29
Migration from SecureWay Directory Version 3.2.2 for Windows InstallShield GUI installations . . . 30
Migration from SecureWay Directory Version 3.2.2 for AIX installations 33
Migration from SecureWay Directory Version 3.2.2 for Solaris and Linux installations 35
Migration from IBM Directory Server version 4.1 or 5.1 for Windows installations 37
Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations 37
  Migrating from IBM Directory Server 4.1 . . . 37
  Migrating from IBM Directory Server 5.1 with DB2 8.1, 32-bit 38
  Migrating from IBM Directory Server 5.1 with DB2 7.2. 39
Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations. 42
Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express. 43
  For Windows installations 43
  For UNIX installations. 44
  For zSeries Linux installations 45

Chapter 6. Installing using the InstallShield GUI 49
Installing on a Windows platform 49
  Before you install 49
  Installing IBM Tivoli Directory Server on a Windows platform 50
Installing on a UNIX-based platform 53
  Before you install 53
  Installing IBM Tivoli Directory Server on a UNIX-based platform 54

Chapter 7. Installing IBM Tivoli Directory Server using AIX utilities . . 57
Before installing on a node within an RS/6000 SP environment 58
SMIT installation 58
Command line installation using installp 60
Installing GSKit 61
  Setting system variables for AIX operating systems. 62
  Removing GSKit. 62

Chapter 8. Installing IBM Tivoli Directory Server using Linux utilities. . 63
Installing IBM Tivoli Directory Server 63
Installing GSKit 65
  Removing GSKit. 65

© Copyright IBM Corp. 1998, 2003

Chapter 9. Installing IBM Tivoli Directory Server using Solaris utilities . 67
Installing IBM Tivoli Directory Server 67
  Package dependencies 67
  "Non-IBM version of LDAP" on your system . . 68
  AdminTool installation 68
  Command line installation using pkgadd . . . 69
Installing GSKit 71
  Removing GSKit. 72

Chapter 10. Installing IBM Tivoli Directory Server using HP-UX utilities . 73
Before installing IBM Tivoli Directory Server . . . 73
  Setting the current kernel configuration parameters 73
Installing IBM Tivoli Directory Server 74
Installing GSKit 75
  Setting system variables for HP-UX 76
  Removing GSKit. 76

Chapter 11. Installing on Windows platforms using silent installation . . . 77
Silent installation 77
  Verifying the silent installation 78
  Options file for silent installation 79
Installing GSKit on Windows operating systems . . 80
  Removing GSKit. 81

Chapter 12. Configuration 83
Using the IBM Tivoli Directory Server Configuration Tool (ldapxcfg) 83
  Setting the Administrator DN and password . . 84
  Configuring or unconfiguring the database . . . 85
  Enabling or disabling the change log 87
  Managing suffixes 88
  Managing schema files 89
  Importing and exporting LDIF data 90
  Backing up, restoring, and optimizing the database 91
Using the ldapcfg utility 92
  Setting the administrator DN and password . . 93
  Configuring the database. 93
  Changing the DB2 administrator password . . . 95
  Enabling the change log 95
  Adding a suffix 95
Importing or exporting data 95
Backing up, restoring, and optimizing the database 95
  Backing up the database using the dbback command 96
  Restoring the database using the dbrestore command 96
  Optimizing the database using the runstats command 96

Chapter 13. After you install and configure. 97
Starting the directory server 97
Starting the application server to use the Web Administration Tool 97
Stopping the application server. 97
Starting the Web Administration Tool. 97

Chapter 14. Unconfiguring the database and uninstalling IBM Tivoli Directory Server. 99
Unconfiguring the database 99
Uninstalling IBM Tivoli Directory Server 100
  Uninstalling using the InstallShield GUI . . . 100
  Uninstalling using operating system utilities . . 101

Chapter 15. Troubleshooting 105
InstallShield GUI installation 105
  Failed installation 106
  Recovering from a failed installation 106
Configuration 107
  DB2 license file expired 107
  Translated titles might truncate in Configuration Tool 108
  Interrupting Configuration Tool database tasks causes an incorrect status for the files 108
  Java failure when configuring an existing instance and database 109
  Error when starting the Configuration Tool on AIX 109
  Configuration programs terminate on AIX. . . 109
  DB2 does not configure properly 109
  Database performance is poor 110
  Server does not start after making changes to configuration files attributes 110
  Transaction log is full. 110
  Configuration Tool 110
Debugging 111
  Error opening slapd.cat on Windows 111
  Logging on to the Web Administration Tool console on Internet Explorer 111
  Corruption of data entered in Web Administration Tool 111
  DB2 errors logged 112
  Server debug mode 113
  Verifying that AIX hardware is 64-bit 115
  Verifying that the AIX kernel is 64-bit 115
  Error on AIX 5.1 when running db2start . . . 115
  Error when starting the embedded version of WebSphere Application Server - Express on AIX. 116
Migration. 116
Web browser problems 117
  Microsoft Internet Explorer 117

Appendix A. Database configuration planning 119

Appendix B. Support for additional locales on UNIX platforms 121

Appendix C. Migrating replication servers 123

Appendix D. Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express 125
Manually installing and configuring the embedded version of WebSphere Application Server - Express. 125
  Installing the embedded version of WebSphere Application Server - Express 125
  Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express 125
Uninstalling the Web Administration Tool from the embedded version of WebSphere Application Server - Express 126
Default ports for the embedded version of WebSphere Application Server - Express 126
Using HTTPS for the embedded version of WebSphere Application Server - Express Version V5.0.2 127

Appendix E. Installing the Web Administration Tool into WebSphere . 129

Appendix F. Installing and configuring DSML. 131

Appendix G. Loading a sample database 133

Appendix H. UTF-8 support 135
Why choose anything other than UTF-8? 135
Server utilities 135
  Examples. 135
Supported IANA character sets 136

Appendix I. Setting up GSKit to support CMS key databases 139

Appendix J. Configuring the database in a location other than /home when /home is an NFS mount 141

Appendix K. IBM Tivoli Directory Server configuration schema 143
Directory Information Tree 143
  cn=Configuration 143
  cn=Admin 144
  cn=AdminGroup 145
  cn=Event Notification 145
  cn=Front End 145
  cn=Kerberos. 146
  cn=Master Server 146
  cn=Referral 147
  cn=Schemas 147
  cn=IBM Directory 147
  cn=Config Backends 148
  cn=ConfigDB 148
  cn=RDBM Backends 149
  cn=Directory 149
  cn=Change Log 150
  cn=LDCF Backends 151
  cn=SchemaDB 151
  cn=SSL 152
  cn=CRL 152
  cn=Transaction 153
  cn=Digest 153
  cn=admin audit 154
  cn=Audit. 154
  cn=Connection Management 155
Attributes 155
  cn 158
  ibm-slapdACLCache 158
  ibm-slapdACLCacheSize 158
  ibm-slapdAdminDN 158
  ibm-slapdAdminGroupEnabled 159
  ibm-slapdAdminPW 159
  ibm-slapdAllowAnon. 159
  ibm-slapdAllReapingThreshold 159
  ibm-slapdAnonReapingThreshold 160
  ibm-slapdBoundReapingThreshold 160
  ibm-slapdBulkloadErrors 160
  ibm-slapdCachedAttribute 161
  ibm-slapdCachedAttributeSize. 161
  ibm-slapdChangeLogMaxAge 161
  ibm-slapdChangeLogMaxEntries 161
  ibm-slapdCLIErrors 162
  ibm-slapdConcurrentRW 162
  ibm-slapdDB2CP 162
  ibm-slapdDBAlias 163
  ibm-slapdDbConnections 163
  ibm-slapdDbInstance 163
  ibm-slapdDbLocation. 164
  ibm-slapdDbName 164
  ibm-slapdDbUserID 164
  ibm-slapdDbUserPW 164
  ibm-slapdDerefAliases 165
  ibm-slapdDigestAdminUser 165
  ibm-slapdDigestAttr 165
  ibm-slapdDigestRealm 166
  ibm-slapdEnableEventNotification 166
  ibm-slapdEntryCacheSize 166
  ibm-slapdErrorLog 167
  ibm-slapdESizeThreshold 167
  ibm-slapdEThreadActivate 167
  ibm-slapdEThreadEnable 168
  ibm-slapdETimeThreshold 168
  ibm-slapdFilterCacheBypassLimit. 168
  ibm-slapdFilterCacheSize 168
  ibm-slapdIdleTimeOut 169
  ibm-slapdIncludeSchema 169
  ibm-slapdSslKeyRingFilePW 170
  ibm-slapdKrbAdminDN. 170
  ibm-slapdKrbEnable 170
  ibm-slapdKrbIdentityMap 171
  ibm-slapdKrbKeyTab 171
  ibm-slapdKrbRealm 171
  ibm-slapdLanguageTagsEnabled 172
  ibm-slapdLdapCrlHost 172

ibm-slapdLdapCrlPassword 172
ibm-slapdLdapCrlPort 173
ibm-slapdLdapCrlUser 173
ibm-slapdMasterDN 173
ibm-slapdMasterPW 174
ibm-slapdMasterReferral 174
ibm-slapdMaxEventsPerConnection 175
ibm-slapdMaxEventsTotal 175
ibm-slapdMaxNumOfTransactions 175
ibm-slapdMaxOpPerTransaction 175
ibm-slapdMaxPendingChangesDisplayed . . . 176
ibm-slapdMaxTimeLimitOfTransactions. . . . 176
ibm-slapdPagedResAllowNonAdmin 176
ibm-slapdPagedResLmt 177
ibm-slapdPageSizeLmt 177
ibm-slapdPlugin 178
ibm-slapdPort 178
ibm-slapdPWEncryption. 179
ibm-slapdReadOnly 179
ibm-slapdReferral 179
ibm-slapdReplDbConns 179
ibm-slapdReplicaSubtree 180
ibm-slapdSchemaAdditions. 180
ibm-slapdSchemaCheck 180
ibm-slapdSecurePort 181
ibm-slapdSecurity 181
ibm-slapdServerId. 181
ibm-slapdSetenv 182
ibm-slapdSizeLimit 182
ibm-slapdSortKeyLimit 182
ibm-slapdSortSrchAllowNonAdmin 183
ibm-slapdSslAuth 183
ibm-slapdSslCertificate 184
ibm-slapdSslCipherSpec 184
ibm-slapdSslFIPsModeEnabled 185
ibm-slapdSslKeyDatabase 185
ibm-slapdSslKeyDatabasePW 185
ibm-slapdSslKeyRingFile 186
ibm-slapdStartupTraceEnabled. 186
ibm-slapdSuffix. 186
ibm-slapdSupportedWebAdmVersion 186
ibm-slapdSysLogLevel 187
ibm-slapdTimeLimit 187
ibm-slapdTraceMessageLevel 187
ibm-slapdTraceMessageLog. 188
ibm-slapdTransactionEnable 188
ibm-slapdUseProcessIdPw 188
ibm-slapdVersion 189
ibm-slapdWriteTimeout 189
objectClass 189

Appendix L. Notices 191
Trademarks 192

Index 195

Preface

This document describes how to install, configure, and uninstall IBM® Tivoli® Directory Server version 5.2. IBM Tivoli Directory Server 5.2 is supported on Windows®, AIX®, Linux (xSeries®, zSeries®, pSeries™, and iSeries™), Solaris, and Hewlett-Packard UNIX® (HP-UX) operating system platforms. For detailed information about supported operating system versions, as well as other required software and hardware, see Chapter 4, “System requirements”, on page 13.

Who should read this book

This book is intended for system administrators.

Publications

Read the descriptions of the IBM Tivoli Directory Server library to determine which publications you might find helpful. After you determine the publications you need, see “Accessing publications online” on page viii.

IBM Tivoli Directory Server library

The publications in the IBM Tivoli Directory Server library are:

IBM Tivoli Directory Server Version 5.2 Readme Addendum
Go to the Tivoli Software Library Web site to access the *IBM Tivoli Directory Server Version 5.2 Readme Addendum*, which contains important information that was not included in the Readme files. See “Accessing publications online” on page viii for information about accessing online publications.

IBM Tivoli Directory Server Version 5.2 Client Readme
Contains last-minute information about the client.

IBM Tivoli Directory Server Version 5.2 Server Readme
Contains last-minute information about the server.

IBM Tivoli Directory Server Version 5.2 Web Administration Tool Readme
Contains last-minute information about the Web Administration Tool. This Readme is available from the main panel of the Web Administration Tool.

IBM Tivoli Directory Server Version 5.2 Installation and Configuration Guide
Contains complete information for installing the IBM Tivoli Directory Server client, server, and Web Administration Tool. Includes information about migrating from a previous version of IBM Tivoli Directory Server or SecureWay Directory.

IBM Tivoli Directory Server Version 5.2 Tuning Guide
Contains information about tuning the server for better performance.

IBM Tivoli Directory Server Version 5.2 Administration Guide
Contains instructions for performing administrator tasks through the Web Administration Tool or the command line.

IBM Tivoli Directory Server Version 5.2 Plug-ins Reference
Contains information about writing server plug-ins.

IBM Tivoli Directory Server Version 5.2 C-Client SDK Programming Reference
Contains information about writing LDAP client applications.

© Copyright IBM Corp. 1998, 2003

Related publications

Information related to the IBM Tivoli Directory Server is available in the following publications:

- IBM Tivoli Directory Server Version 5.2 uses the Java Naming and Directory Interface (JNDI) client from Sun Microsystems. For information about the JNDI client, refer to the *Java Naming and Directory Interface™ 1.2.1 Specification* on the Sun Microsystems Web site at http://java.sun.com/products/jndi/1.2/javadoc/index.html.
- The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at: http://www.ibm.com/software/tivoli/library/
- The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available, in English only, from the **Glossary** link on the left side of the Tivoli Software Library Web page http://www.ibm.com/software/tivoli/library/

Accessing publications online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli software library: http://www.ibm.com/software/tivoli/library.

To locate product publications in the library, click the **Product manuals** link on the left side of the library page. Then, locate and click the name of the product on the Tivoli software information center page.

Information is organized by product and includes READMEs, installation guides, user's guides, administrator's guides, and developer's references.

Note: To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe Acrobat Print window (which is available when you click **File → Print**).

Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. After installation, you also can use the keyboard instead of the mouse to operate all features of the graphical user interface.

Contacting software support

Before contacting IBM Tivoli Software support with a problem, refer to Tivoli Software support Web site at:

http://www.ibm.com/software/sysmgmt/products/support/

If you need additional help, contact software support by using the methods described in the *IBM Software Support Guide* at the following Web site:

http://techsupport.services.ibm.com/guides/handbook.html

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers and e-mail addresses, depending on the country in which you are located
- A list of information you should gather before contacting customer support

Conventions used in this book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface conventions

The following typeface conventions are used in this reference:

Bold	Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java classes, and objects are in **bold**.
Italic	Titles of publications, and special words or phrases that are emphasized are in *italic*.
<*Italic*>	Variables are set off with < > and are in <*italic*>.
`Monospace`	Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in `monospace`.

Operating system differences

This book uses the UNIX convention for specifying environment variables and for directory notation. When using the Windows command line, replace *$variable* with *%variable%* for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Chapter 1. Quick installation path

To follow the simplest path through installation, use the checklist in this chapter. If you are migrating from a previous release, do not use this checklist. See Chapter 5, “Migration from previous releases”, on page 29 for instructions.

__ 1. Be sure that you have the minimum required hardware and software.

See Chapter 4, “System requirements”, on page 13 for information. There is a section for the client and the server for each operating system.

Also see the *IBM Tivoli Directory Server Version 5.2 Server Readme*, *IBM Tivoli Directory Server Version 5.2 Client Readme*, and *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See “Accessing publications online” on page viii for information about accessing online publications.)

__ 2. Plan your database.

See Appendix A, “Database configuration planning”, on page 119 for information.

__ 3. If you are installing the server, create the user ID that will own the database. (On UNIX-based platforms, you can wait until after installation, but you must create the user ID before configuration.)

See “Before you configure: creating the DB2 database owner and database instance owner” on page 85 for information.

__ 4. Install IBM Tivoli Directory Server using the InstallShield GUI, if available for your operating system platform. You can use the InstallShield GUI on Windows, AIX, xSeries Linux, and Solaris operating systems.

For Windows platforms, see “Installing on a Windows platform” on page 49.

For UNIX-based platforms, see “Installing on a UNIX-based platform” on page 53.

Note: If you prefer to install IBM Tivoli Directory Server using utilities for your operating system, see the chapter for your operating system. These chapters are:

- Chapter 7, “Installing IBM Tivoli Directory Server using AIX utilities”, on page 57
- Chapter 8, “Installing IBM Tivoli Directory Server using Linux utilities”, on page 63
- Chapter 9, “Installing IBM Tivoli Directory Server using Solaris utilities”, on page 67
- Chapter 10, “Installing IBM Tivoli Directory Server using HP-UX utilities”, on page 73

__ 5. On Windows, after the system restarts, log on as the user you were logged on as during installation.

__ 6. After the Configuration Tool starts, set the Administrator distinguished name (DN) and password.

See “Setting the Administrator DN and password” on page 84 for information.

© Copyright IBM Corp. 1998, 2003

Note: If you used operating system utilities to install, you must start configuration from the command line, using one of the following commands:

- **ldapxcfg** to use the Configuration Tool.
- **ldapcfg** to use the command line utility. See "Using the ldapcfg utility" on page 92 for information.

__ 7. Configure the database using the Configuration Tool.

See "Configuring the database" on page 86 for information.

__ 8. Optionally, verify the installation and configuration by loading the sample database.

See Appendix G, "Loading a sample database", on page 133 for information.

__ 9. Start the server and the Web Administration Tool.

See Chapter 13, "After you install and configure", on page 97 for information.

__ 10. See the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for information about setting up and using the server.

Chapter 2. About this release

This chapter gives detailed information about new features and industry standards that are implemented in this release of IBM Tivoli Directory Server.

What's new for this release

The following enhancements and changes have been made to IBM Tivoli Directory Server for the 5.2 release.

Updated versions of corequisite products

The InstallShield GUI installation program includes an integrated installation of the following products. These products are also available on the CD or they can be downloaded.

- DB2® Universal Database version 8.1 Enterprise Server Edition (DB2) with FixPak 2.
- Global Security Kit (GSKit) version 7a. GSKit includes open-source libraries.
- The embedded version of WebSphere Application Server - Express version 5.0.2.

Support for Windows Server 2003

IBM Tivoli Directory Server supports the Microsoft® Windows Server 2003 operating system, Standard and Enterprise editions.

Non-SSL packages only on AIX

In previous versions, both Secure Sockets Layer (SSL) and non-SSL packages were provided on all operating system platforms. For IBM Tivoli Directory Server version 5.2, non-SSL packages are provided only on AIX.

Full 64-bit server support on AIX

IBM Tivoli Directory Server has been ported to 64-bit architecture on AIX only. Solaris, HP-UX, Linux zSeries, Linux Intel, Linux iSeries and pSeries, and Windows remain 32-bit servers. The Web Administration Tool remains a 32-bit application. The 32-bit server will no longer be available on AIX; however, the client SDK will still be available as a 32-bit application. The 64-bit architecture increases the ability to cache a large number of directory entries.

Notes:

1. AIX Version 5.1 or later is required for the 64-bit AIX Server.
2. To move up to 64-bit server support, you must migrate your database. However, you do not need to unload and reload your data. See Chapter 5, "Migration from previous releases", on page 29 for information.

Authentication methods for LDAP (RFC 2829)

IBM Tivoli Directory Server 5.2 provides support for DIGEST-MD5 Simple Authentication and Security Layer (SASL) authentication, as well as Transport Layer Security (TLS) support as defined in RFC 2829.

LDAP v3 Extensions for TLS (RFC 2830)

TLS allows clients to connect to the server on a non-secure port and issue a TLS start command. If GSKit is installed, the server

© Copyright IBM Corp. 1998, 2003

honors the request and begins a secure connection with the client. RFC 2830 specifies how LDAP should support TLS.

DIGEST-MD5 SASL Mechanism (RFC 2831)
RFC 2831 defines how HTTP Digest Authentication (Digest) can be used as an SASL mechanism for any protocol that has an SASL profile. (RFC 2222 defines SASL.) DIGEST-MD5 is intended to be both an improvement over CRAM-MD5 and a convenient way to support a single authentication mechanism for Web, mail, LDAP, and other protocols.

Use of Language codes (RFC 2596)
RFC 2596 defines a mechanism that allows the directory to associate natural language codes with values that meet certain natural language requirements. IBM Tivoli Directory Server 5.2 supports a single language code option and language tag support discovery.

Subtree search on null base
A subtree can now be searched from a null base. This provides a shorthand way to retrieve all entries in the directory. In earlier releases, multiple searches were required for each suffix to search the entire directory.

Unique Attributes
IBM Tivoli Directory Server 5.2 allows the administrator to identify attributes that must have unique values. This ensures that there are not two directory entries with the same attribute values. For example, no two users can have the same user ID or email address if these attributes have been configured to enforce uniqueness.

Delegation of server administration to a group of administrative users
In previous releases, IBM Directory Server required that the administrator user ID be used to perform server tasks such as replication configuration and starting and stopping the server. For the 5.2 release, there is an administration group that contains IDs of users with administrative rights and privileges. This avoids the use of a single administration ID shared by a number of administrators. The root administrator can add or remove members from the administration group.

Prevention of denial of service
For the 5.2 release, support has been added to reduce the vulnerability of the server to malicious attacks, causing a denial of service. The server can be configured to reject non-responsive clients after some number of attempts. Support has also been added to close connections issued by a specific IP address or DN. An emergency thread is available when some number of items, configurable on the server, are on the work queue. This provides a method for the administrator to access the server during a denial of service attack. The oldest connections can, through configurable parameters, be reused first.

Unbind of bound DN/IP
This security enhancement allows an administrator to force a specific bound DN or IP address to unbind. The emergency thread added in the denial of service prevention feature enhances this feature by ensuring that an administrator always has access to unbind bound DNs and IP addresses.

Group specific search limits
You can now configure "extended" search limits for a defined group of people who are not the administrator or part of the administration group.

Preservation of operational attributes

The operational attributes **creatorsName**, **createTimestamp**, **lastModifiedBy**, and **lastModifiedTime** are now preserved so that they are consistent between a master and its replicas. In addition, these attributes are now imported by the **ldif2db** and **bulkload** utilities and exported by the **db2ldif** utility.

Attribute cache

The attribute cache improves search performance for certain search filters by allowing configured attributes and their values to be stored in memory. When a search is performed using a filter that contains all cached attributes and the filter is of a type supported by the attribute cache manager, the filter can be resolved in memory; this leads to improved search performance.

Serviceability improvements

The following new features improve the serviceability of IBM Tivoli Directory Server:

Server input and output logging

The actual input and output from the server can now be logged to allow better analysis of problems. In previous releases, the LDAP client library output the BER data to stderr or a file. The new feature adds the capability to record the same formatted BER data one time to the in-memory trace. The trace facility can then be used to extract this data.

Dynamic trace enablement

Trace information from the server can now be captured without stopping and restarting the server. The level of tracing and the size available for trace output can also be configured dynamically.

Monitor enhancements

More information has been added to the output of **cn=monitor** to be used in analyzing server performance. These attributes are intended for directory administrators only. The new information includes counts of completed operations by type (for example, BIND, MODIFY, COMPARE, SEARCH), depth of the work queue, number of available workers, counts of messages added to the server log, audit log, command-line interface errors, and counts of SSL connections. Information is also included about what worker threads are doing and when they started.

Additional support on iSeries and pSeries Linux

Support for the new iSeries and pSeries Linux platforms was added in the IBM Tivoli Directory Server 5.1 FixPak 1. IBM Tivoli Directory Server 5.2 adds more support for iSeries and pSeries: the Web Administration Tool can now be used on these platforms, and translated messages have been added.

System and restricted ACLs - compatibility with OS/390®

Support has been added for specification and evaluation of ACLs for the system and restricted attribute classes. This resolves the following interoperability problems between IBM Tivoli Directory Server and OS/390 versions of the LDAP Server.

- In previous releases, during replication the IBM Tivoli Directory Server server rejected any directory entry data that contained ACL specifications with references to system or restricted attribute classes.

Replication from an OS/390 server provider to an IBM Tivoli Directory Server server consumer therefore failed.

- In previous releases, ACL management code could not be written that would run correctly on both types of servers. A client application written for an IBM Tivoli Directory Server environment might not work properly on an OS/390 server because the ACLs might not allow the application to read system attributes. Conversely, a client application developed for an OS/390 server environment would fail to work properly on an IBM Tivoli Directory Server server if the application attempted to set ACLs on system or restricted attributes.

This feature replaces the limited restricted attribute class ACL support, originally provided by IBM Directory Server 5.1 Protection of Access Control Information feature (ibm-slapdACLAccess), with full directory specific ACL support. The behavior of this feature is consistent with the existing ACL support provided for the other attribute access classes: normal, sensitive, and critical.

To maintain consistency with the legacy IBM Directory Server ACL model, existing version 5.1 directories that contain entries with explicit ACL specification will be automatically migrated to provide legacy default read, search, and compare access for the subject DN group:cn=anybody, as well as any specific access IDs. This is to prevent an unexpected loss of default access after migration. If denial of access is required, it should be explicitly specified in the directory, based on the specific needs and desires of the individual IBM Tivoli Directory Server administrator.

Support for identity assertions (proxied authentication)

Support has been added for identity assertions, also known as LDAP Proxied Authorization Control. The Proxied Authorization Control allows a client to request that an operation be processed under a provided authorization identity instead of as the current authorization identity associated with the connection.

Option that the server does not dereference aliases by default

In previous releases, the Java™ Naming and Directory Interface (JNDI) had dereferencing aliases by default. This sometimes caused performance degradation on the server even if no alias entries existed in the server. A server configuration option has been added to override the dereference option specified in the client search request. Additionally, if no alias objects exist in the directory, the server always bypasses the dereference logic.

Gateway replication

Gateway replication uses Gateway servers to collect and distribute replication information effectively across a replicating network. The primary benefit of Gateway replication is the reduction of network traffic.

Enhancements to the Web Administration Tool

Enhancements have been made to the Web Administration Tool, including the following:

- Support for administration of OS/400® V5R3 and z/OS™ R4 LDAP servers
- Support for object class inheritance from multiple superior objects
- Support for peer to peer replication
- Support for gateway replication
- Web Administration support for most new features

Support for industry standards

The following standards are implemented in IBM Tivoli Directory Server 5.2. This list includes standards that were implemented in previous releases. Newly implemented standards are marked with an asterisk (*).

- RFC 1274 The COSINE and Internet X.500 Schema
- RFC 1777 Lightweight Directory Access Protocol (V2)
- RFC 1778 String Representation of Standard Attribute Syntaxes
- RFC 1779 String Representation of Distinguished Names
- RFC 1823 LDAP Application Program Interface (V2)
- RFC 2052 A DNS RR for Specifying the Location of Services (DNS SRV)
- RFC 2219 Use of DNS Aliases for Network Services
- RFC 2222 Simple Authentication and Security Layer (SASL)
- RFC 2247 Using Domains in LDAP/X.500 Distinguished Names
- RFC 2251 Lightweight Directory Access Protocol (V3)
- RFC 2252 Lightweight Directory Access Protocol (V3): Attribute Syntax Definitions
- RFC 2253 Lightweight Directory Access Protocol (V3): UTF-8 String Representation of Distinguished Names
- RFC 2254 The String Representation of LDAP Search Filters
- RFC 2255 The LDAP URL Format
- RFC 2256 A Summary of the X.500(96) User Schema for use with LDAPv3
- * RFC 2596 Use of Language code in LDAP
- RFC 2696 LDAP Control Extension for Simple Paged Results Manipulation
- * RFC 2829 Authentication Methods for LDAP
- * RFC 2830 (V3) Extension for Transport Layer Security (TLS)
- * RFC 2831 Using DIGEST authentication as a SASL Mechanism
- RFC 2849 The LDAP Data Interchange Format (LDIF) - Technical Specification
- RFC 2891 LDAP Control Extension for Server Side Sorting of Search Results
- The Open Group schema for liPerson and liOrganization (NAC/LIPS)

Chapter 3. Installation, configuration, and migration overview

This chapter briefly describes the migration, installation, and configuration procedures for IBM Tivoli Directory Server version 5.2.

If you have a pre-existing version of Lightweight Directory Access Protocol (LDAP) from a vendor other than IBM, you should remove it before installing the IBM Tivoli Directory Server. If you attempt to install the IBM Tivoli Directory Server without removing the other vendor's version, the resulting file name conflicts might prevent either version from working.

Note: A version of LDAP is installed by default on some operating systems.

Migration from a previous release

If you have a previous version of the IBM Directory, such as SecureWay® Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1, 5.1, or 5.1 for Linux iSeries and pSeries, migration is necessary to preserve any changes that you have made to the schema definitions and to preserve your directory server configuration.

If you want to migrate your data, see Chapter 5, "Migration from previous releases", on page 29 before beginning the installation process for IBM Tivoli Directory Server 5.2.

Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, or 3.2.1 currently installed and you want to migrate your data, you must upgrade to level 3.2.2 before installing IBM Tivoli Directory Server 5.2. You can download SecureWay Directory version 3.2.2 from the IBM Directory Web page at http://www.ibm.com/software/tivoli/products/directory-server/

See the SecureWay Directory version 3.2.2 documentation for information about migrating from version 3.1.1.5.

Before you install: zip, tar, and iso files

The IBM Tivoli Directory Server product is available in three file formats: zip, tar, and iso.

If you downloaded a zipped file, use a product such as PKZIP to unzip the file after you download it to your computer.

The tar file is a Tape ARchive type of file. After you download a tar file, untar it.

The iso version of the product is used to burn an installation CD-ROM that can then be used in the installation process. The iso file is an image that must be processed through a CD-ROM burner program to create the CD-ROM. When you create the CD-ROM, be sure that you do not make a data CD of the iso file. Select the option that unencapsulates the data from the iso file and burns the files on the CD-ROM.

After you process the downloaded file, you can install IBM Tivoli Directory Server using the installation instructions in the appropriate installation chapter.

© Copyright IBM Corp. 1998, 2003

Installation

When you install IBM Tivoli Directory Server, you can install either the client or the server, which requires the client.

In addition, you can install the Web Administration Tool on an application server, with or without the server or the client. You can use the Web Administration Tool to administer IBM Tivoli Directory Server servers either locally or remotely. You can install a single Web Administration console to manage multiple IBM Tivoli Directory Server servers. (You can manage servers from previous releases, including SecureWay Directory 3.2.x and IBM Directory Server version 4.1 and 5.1. See "Requirements for the Web Administration Tool" on page 26 for a complete list of servers that can be managed.)

IBM Tivoli Directory Server 5.2 has several installation options. You can install using an InstallShield graphical user interface (GUI) or use platform-specific installation methods such as the command line or installation tools for the operating system. Instructions for using the InstallShield GUI are found in Chapter 6, "Installing using the InstallShield GUI", on page 49.

For platform-specific installation instructions, see the installation chapter for the platform for which you are installing. For example, see Chapter 7, "Installing IBM Tivoli Directory Server using AIX utilities", on page 57.

Note: Only native installation methods are available for HP-UX; iSeries, pSeries, and zSeries Linux operating systems; and AIX 4.3.3 (client only).

See Chapter 4, "System requirements", on page 13 for hardware and software requirements.

Configuration

You can use either the Configuration Tool (**ldapxcfg**), which has a GUI, or the **ldapcfg** command-line utility to configure the server. To unconfigure the server, you can use **ldapxcfg** or the **ldapucfg** command-line utility.

After successful installation of the server, if you used the InstallShield GUI to install, the Configuration Tool runs. (This is true for all platforms on which the InstallShield GUI is supported.) If you did not use the InstallShield GUI to install, you must run the Configuration Tool or use **ldapcfg**. You must perform the following configuration tasks before you can use the server:

- Set the IBM Tivoli Directory Server administrator distinguished name (DN) and password. This operation can be compared to defining the root user ID and password on a UNIX system.
- Configure the database. (Be sure that you have created the user ID for the database owner first. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for detailed information.)

The **ldapxcfg** program can be used for the following tasks:

- Setting or changing the IBM Tivoli Directory Server administrator distinguished name (DN) and password
- Configuring and unconfiguring the database
- Enabling and disabling the changelog
- Adding or removing suffixes

- Adding schema files to or removing schema files from the list of schema files to be loaded at startup
- Importing and exporting LDAP Data Interchange Format (LDIF) data
- Backing up, restoring, and optimizing the database

If you prefer to use the command line, all the tasks in the list can be done with a combination of command line utilities, including **ldapcfg**, **ldapucfg**, **dbback**, **dbrestore**, **runstats**, **bulkload**, **ldif2db**, and **db2ldif**.

You can find information about **ldapxcfg**, **ldapcfg**, **ldapucfg**, **dbback**, **dbrestore**, and **runstats** in Chapter 12, “Configuration”, on page 83 and Chapter 14, “Unconfiguring the database and uninstalling IBM Tivoli Directory Server”, on page 99.

Chapter 4. System requirements

To install the IBM Tivoli Directory Server packages, administer the server, and use the Global Security Kit (GSKit), your computer must meet the minimum system requirements as outlined in this chapter.

Requirements for the client

The following sections show system requirements for the IBM Tivoli Directory Server client.

Windows operating systems client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of Windows operating systems. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped the client package. After installing, the client Readme file is located in the *installpath*\doc\lang directory in files client.txt, client.pdf, and client.htm, where:

- *lang* is the locale you chose when you installed IBM Tivoli Directory Server.
- *installpath* is the location where the IBM Tivoli Directory Server client is installed.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the Windows client:

Operating system

The client is supported on the following Windows operating system platforms:

- Microsoft Windows 2000
- Windows XP
- Windows Server 2003 Standard or Enterprise
- Windows NT® 4.0 with Service Pack 6 or higher

Memory

A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Disk space

If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the directory specified by the TEMP environment variable.

Other software

To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

AIX operating system client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of the AIX operating system.

© Copyright IBM Corp. 1998, 2003

The file name is client.txt. The file is in the root directory of the CD or the directory where you untarred the client package. After installing, the client Readme file is located in the /usr/ldap/doc/*lang* directory in files client.txt, client.pdf, and client.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the AIX client:

Operating system

The client is supported on the following versions of AIX:

- AIX 4.3.3
- AIX 5.1
- AIX 5.2

Note: The client is 32-bit.

Memory

A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Disk space

If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and at least 200 MB in the /tmp directory.

Note: The InstallShield GUI is not available on AIX 4.3.3.

Other software

- The Korn shell is required.
- For AIX 4.3.3 you must install AIX Maintenance Level 8 or higher. On AIX 5.1, you must install AIX Maintenance Level 4 or higher. On AIX 5.2, you must install AIX Maintenance Level 1 or higher.

  Note: If you have no locale-specific requirements, after you apply all the services that you need for your system, restart your system to enable the changes.
- The bos.loc.iso.ZH_TW fileset must be installed for the Taiwan locale. The fileset is available from the AIX 4.3.3 installation medium.
- The xlC.rte 6.0.0.0 or later fileset is required for GSKit 7a on AIX 5.1 and 5.2.
- The xlC.aix43.rte 6.0.0.0 or later fileset is required for GSKit 7a on AIX 4.3.3.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

xSeries Linux operating system client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of the Linux operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you untarred the client package. After installing, the client Readme file is located in the /usr/ldap/doc/*lang* directory in files client.txt, client.pdf, and client.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the xSeries Linux client:

Operating system
The client is supported on the following versions of xSeries Linux:
- Red Hat Enterprise Linux 3.0
- UnitedLinux 1.0
- SuSE Linux Enterprise Server 8

Memory
A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Disk space
If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and at least 200 MB in the /tmp directory.

Other software
- The Korn shell is required.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

zSeries Linux operating system client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of the zSeries Linux operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you untarred the client package. After installing, the client Readme file is located in the /usr/ldap/doc/*lang* directory in files client.txt, client.pdf, and client.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the zSeries Linux client:

Operating system
The client is supported on the following versions of zSeries Linux:
- Red Hat Enterprise Linux 3.0
- SuSE Linux Enterprise Server 8

Memory
A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Other software
- The Korn shell is required.

- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

iSeries and pSeries Linux operating system client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of the iSeries or pSeries Linux operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you untarred the client package. After installing, the client Readme file is located in the /usr/ldap/doc/*lang* directory in files client.txt, client.pdf, and client.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the iSeries and pSeries for Linux clients:

Operating system
The client is supported on the following versions of iSeries and pSeries for Linux:

- Red Hat Enterprise Linux 3.0
- UnitedLinux 1.0
- SuSE Linux Enterprise Server 8

Memory
A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Other software

- The Korn shell is required.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

Solaris operating system client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of the Solaris operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you untarred the client package. After installing, the client Readme file is located in the /opt/IBMldaps/doc/*lang* directory in files client.txt, client.pdf, and client.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the Solaris client:

Operating system
The client is supported on the following versions of Solaris:

- Solaris Operating Environment™ Software versions 7, 8, or 9

Memory

A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Disk space

If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and at least 200 MB in the /tmp directory.

Other software

- The Korn shell is required.
- Ensure that the code page conversion routines (en_US.UTF-8 1.0) are installed.
- If you plan to use the InstallShield GUI to install, patches are required for the Java 2 Runtime Environment, v. 1.4.1.

  To obtain patches, see the SunSolve support Web site at:

  http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE.

  Also see http://java.sun.com/j2se/1.3/font-requirements.html for information about which font packages should be on your system.
- To use GSKit, the following are required:
  - On Solaris 7, the following patches are required for the gsk runtime and SDK 2: 106950-22, 106327-18, 106300-19, 107834-04, 107544-03, 106541-24, and 106980-22.
  - On Solaris 8, the following patches are required for the gsk runtime: 108434-02 111327-02, 108991, 108827 and 108528 For gsk SDK 2 : 109505-08, 109508-04, 109510-03, and 109513-05.
  - On Solaris 9, the following patches are required for the gsk runtime: 108434-02 111327-02, 108991, 108827 and 108528. The following patches are required for the gsk SDK 2: 109505-08, 109508-04, 109510-03, and 109513-05.
  - IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

Hewlett-Packard UNIX (HP-UX) operating system client requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Client Readme* for any updated information about supported versions of the HP-UX operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you untarred the client package. After installing, the client Readme file is located in the /usr/IBMldap/doc/*lang* directory in files client.txt, client.pdf, and client.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See “Accessing publications online” on page viii for information about accessing online publications.)

The following hardware and software are required for the HP-UX client:

Operating system

The client is supported on HP-UX 11 or 11i with the following patches:

- December 2001 GOLDBASE11i bundle
- December 2001 GOLDAPPS11i bundle
- Patch PHSS_26560

Memory

A minimum of 128 MB RAM is required. (For better results, use 256 MB or more.)

Other software

- The Korn shell is required.
- To use GSKit, HP-UX Runtime Environment for the Java 2 Platform Version 1.4.1. is required.
- To use GSKit, the following patches are required:
  - For HP-UX 11, patches 108434-02 111327-02, 108991, 108827 and 108528 are required for the gsk runtime; patches 109505-08, 109508-04, 109510-03, and 109513-05 are required for the gsk SDK.
  - For HP-UX 11i, patch PHSS_26946 is required for the gsk runtime.

Requirements for the server (including the client)

The following sections show system requirements for installing and using the server. These requirements include the client requirements.

Windows operating systems server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of the Windows operating system. The Readme file is in the root directory of the CD or the directory where you unzipped the server package. After installing, the Readme file is located in the *installpath*\doc*lang* directory in files server.txt, server.pdf, and server.htm, where:

- *installpath* is the location where IBM Tivoli Directory Server is installed.
- *lang* is the locale you chose when you installed IBM Tivoli Directory Server. For example, for United States English the locale is en_US.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the Windows server:

Operating system

The server is supported on the following versions of Windows:

- Windows 2000
- Windows Server 2003, Standard or Enterprise
- Windows NT 4.0 with Service Pack 6 or later; a Windows NT file system (NTFS) is required for security support.

Memory

A minimum of 256 MB RAM is required. (For better results, use 512 MB or more.)

Disk space

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the directory specified by the TEMP environment variable.
- If you already have DB2 installed, you need approximately 25 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 110 MB.

- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on Windows systems. Also allow another 2 to 3 MB of disk space when creating the DB2 instance. See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other software

- The minimum supported level of DB2 is DB2 Version 7.2 with FixPak 5 or later. DB2 Version 8.1 Enterprise Server Edition with FixPak 2 is included with IBM Tivoli Directory Server and is installed if a supported version of DB2 is not detected on your system. If you have a version of DB2 earlier than Version 7.2 with FixPak 5 installed on your system, you must remove it or upgrade it before installing IBM Tivoli Directory Server version 5.2.

  Attention: If you have a version of SecureWay Directory installed, read and understand the migration process in Chapter 5, "Migration from previous releases", on page 29 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

AIX operating system server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of the AIX operating system. The file name is server.txt. The file is in the root directory of the CD or the directory where you untarred the server package. After installing, the Readme file is located in the /usr/ldap/doc/*lang* directory in files server.txt, server.pdf, and server.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the AIX server:

Operating system

The server is supported on the following versions of AIX:

- AIX 5.1
- AIX 5.2

Note: The server is not supported on AIX 4.3.3.

Memory

A minimum of 512 MB RAM is required. (For better results, use 1 GB or more.)

Disk space

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and at least 400 MB in the /tmp directory.
- If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2

requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 160 MB.

- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also, ensure that there is approximately another 4 MB of disk space in the home directory of the user who will own the database to create the DB2 instance. (Normally, this directory is /home, but you can specify another directory if you do not have enough space in the /home directory. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for more information.) See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other hardware

You must be running on 64-bit hardware. See "Verifying that AIX hardware is 64-bit" on page 115 for information about detecting whether your hardware is 64-bit.

Other software

- You must be running a 64-bit kernel. See "Verifying that the AIX kernel is 64-bit" on page 115 for information about detecting whether you are running a 64-bit kernel.
- The Korn shell is required.
- On AIX 5.1, you must install AIX Maintenance Level 4 or higher. On AIX 5.2, you must install AIX Maintenance Level 1 or higher.

  Note: If you have no locale-specific requirements, after you apply all the services that you need for your system, restart your system to enable the changes.
- The xlC.aix50.rte 6.0.0.0 or later fileset is required for GSKit 7a.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

Other Be sure that asynchronous I/O is turned on. See "Error on AIX 5.1 when running db2start" on page 115 for information.

- DB2 Universal Database for AIX version 8.1 Enterprise Server Edition with FixPak 2 (DB2) is included with the IBM Tivoli Directory Server. For AIX, no previous versions of DB2 are supported.

  Notes:

  1. If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 or 5.1 installed, read and understand the migration process in Chapter 5, "Migration from previous releases", on page 29 before removing or upgrading DB2.
  2. If you are upgrading your level of DB2, ensure that you follow the DB2 migration procedure, which requires you to stop all applications. If you have a server up and running and you uninstall DB2 without reinstalling the IBM Tivoli Directory Server, the directory server cannot start.

xSeries Linux operating system server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of Linux. The file name is server.txt. The file is in the root directory of the CD or the directory where you untarred the server package. After installing, the server Readme file is located in the /usr/ldap/doc/*lang* directory in files server.txt, server.pdf, and server.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the xSeries Linux server:

Operating system

The server is supported on the following versions of xSeries Linux:

- UnitedLinux 1.0 (including SP2)
- SuSE Linux Enterprise Server 8
- Red Hat Enterprise Linux 3.0

Memory

A minimum of 256 MB RAM is required. (For better results, use 512 MB or more.)

Disk space

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and at least 400 MB in the /tmp directory.
- If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 160 MB.
- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also allow approximately another 4 MB of disk space in the home directory of the user who will own the database to create the DB2 instance. (Normally, this directory is /home, but you can specify another directory if you do not have enough space in the /home directory. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for more information.) See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other software

- The Korn shell is required.
- DB2 Universal Database for Linux version 8.1 Enterprise Server Edition with FixPak 2 (DB2) is included with the IBM Tivoli Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

  Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 or 5.1 installed, read and understand the migration process in Chapter 5, "Migration from previous releases", on page 29 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

zSeries Linux operating system server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of zSeries Linux. The file name is server.txt. The file is in the root directory of the CD or the directory where you untarred the server package. After installing, the server Readme file is located in the /usr/ldap/doc/*lang* directory in files server.txt, server.pdf, and server.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the zSeries Linux server:

Operating system

The server is supported on the following versions of zSeries Linux:

- SuSE Linux Enterprise Server 8
- Red Hat Enterprise Server 3.0

Memory

A minimum of 256 MB RAM is required. (For better results, use 512 MB or more.)

Disk space

- If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 160 MB.
- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also allow approximately another 4 MB of disk space in the home directory of the user who will own the database to create the DB2 instance. (Normally, this directory is /home, but you can specify another directory if you do not have enough space in the /home directory. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for more information.) See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other software

- The Korn shell is required.
- DB2 Universal Database for Linux version 8.1 Enterprise Server Edition with FixPak 2 (DB2) is included with the IBM Tivoli Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

  Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 or 5.1 installed, read and understand the migration process in Chapter 5, "Migration from previous releases", on page 29 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.
- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

iSeries and pSeries Linux operating system server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of iSeries and pSeries Linux. The file name is server.txt. The file is in the root directory of the CD or the directory where you untarred the server package. After installing, the server Readme file is located in the /usr/ldap/doc/*lang* directory in files server.txt, server.pdf, and server.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the iSeries and pSeries Linux servers:

Operating system

The server is supported on the following versions of iSeries and pSeries Linux:

- Red Hat Enterprise Server 3.0
- SuSE Linux Enterprise Server 8.

Memory

A minimum of 256 MB RAM is required. (For better results, use 512 MB or more.)

Disk space

- If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 160 MB.
- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also allow approximately another 4 MB of disk space in the home directory of the user who will own the database to create the DB2 instance. (Normally, this directory is /home, but you can specify another directory if you do not have enough space in the /home directory. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for more information.) See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other software

- The Korn shell is required.
- DB2 Universal Database for Linux version 8.1 Enterprise Server Edition with FixPak 2 (DB2) is included with the IBM Tivoli Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

  Attention: If you have IBM Directory Server 5.1 for Linux iSeries and pSeries installed, read and understand the migration process in Chapter 5, "Migration from previous releases", on page 29 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.

- To use GSKit, the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

Solaris operating system server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of Solaris. The file name is server.txt. The file is in the root directory of the CD or the directory where you untarred the server package. After installing, the server Readme file is located in the /opt/IBMldaps/doc/*lang* directory in files server.txt, server.pdf, and server.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the Solaris server:

Operating system
The server is supported on the following versions of Solaris:

- Solaris Operating Environment Software versions 8 or 9

Memory
A minimum of 256 MB RAM is required. (For better results, use 512 MB.)

Disk space

- If you plan to use the InstallShield GUI to install, be sure that you have at least 100 MB of free space in the /var directory and at least 400 MB in the /tmp directory.
- If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 160 MB.
- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also allow approximately another 4 MB of disk space in the home directory of the user who will own the database to create the DB2 instance. (Normally, this directory is /home, but you can specify another directory if you do not have enough space in the /home directory. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for more information.) See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other software

- The Korn shell is required.
- Ensure that the code page conversion routines (en_US.UTF-8 1.0) are installed.
- In addition, if you plan to use the InstallShield GUI to install or the Configuration Tool for configuration, patches are required for the Java 2 Runtime Environment, v. 1.4.1.

  To obtain patches, see the SunSolve support Web site at:

  http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE.

Also see http://java.sun.com/j2se/1.3/font-requirements.html for information about which font packages should be on your system.

- DB2 Universal Database for Solaris version 8.1 Enterprise Server Edition with FixPak 2 (DB2) is included with the IBM Tivoli Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

  Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 or 5.1 installed, read and understand the migration process in Chapter 5, "Migration from previous releases", on page 29 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.

  If you use DB2 8.1, the following patches are required:

  - On Solaris 8 (32-bit): "Recommended & Security Patches" + 108921-12 + 108940-24 + 108434-03 and 108528-12
  - On Solaris 8 (64-bit): "Recommended & Security Patches" + 108921-12 + 108940-24 + 108435-03 and 108528-12

  "Recommended & Security Patches" can be obtained from the http://sunsolve.Sun.com Web site. On the SunSolve Online Web site, click the **Patches** menu item in the left-hand panel and select **Recommended & Security Patches** from the **Browse & Download Patches** section.

  The J2SE Solaris Patch Clusters are also required. They can be obtained from the http://sunsolve.Sun.com Web site. From the SunSolve Online Web site, click on the **Patches** menu item in the left-hand panel and select **Recommended & Security Patches** from the **Browse & Download Patches** section.

  The SUNWlibC software is required to install DB2 on Solaris.

  You will need a Java Runtime Environment (JRE) to run the DB2 Java-based tools, such as the Control Center, and to create and run Java applications, including stored procedures and user-defined functions. During the installation process, if the correct level of the JRE is not already installed, it will be installed.

  A browser is required to view online help.

- To use GSKit, the following are required:
  - On Solaris 8, the following patches are required for the gsk runtime: 108434-02 111327-02, 108991, 108827 and 108528 For gsk SDK 2 : 109505-08, 109508-04, 109510-03, and 109513-05.
  - On Solaris 9, the following patches are required for the gsk runtime: 108434-02 111327-02, 108991, 108827 and 108528. The following patches are required for the gsk SDK 2: 109505-08, 109508-04, 109510-03, and 109513-05.
  - The IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK is required.

HP-UX operating system server requirements

Before installing, see the *IBM Tivoli Directory Server Version 5.2 Server Readme* for any updated information about supported versions of HP-UX. The file name is server.txt. The file is in the root directory of the CD or the directory where you untarred the server package. After installing, the server Readme is located in the

/usr/IBMldap/doc/*lang* directory in files server.txt , server.pdf, and server.htm, where *lang* is the locale you chose when you installed IBM Tivoli Directory Server.

Also see the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for last-minute information. (See "Accessing publications online" on page viii for information about accessing online publications.)

The following hardware and software are required for the HP-UX server:

Operating system
The server is supported on HP-UX 11i with the following patches:
- December 2001 GOLDBASE11i bundle
- December 2001 GOLDAPPS11i bundle
- patch PHSS_26560

Memory
A minimum of 512 MB RAM is required.

Disk space
- If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Tivoli Directory Server (including the client and the server) requires about 160 MB.
- Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also, ensure that there is approximately another 4 MB of disk space in the home directory of the user who will own the database to create the DB2 instance. (Normally, this directory is /home, but you can specify another directory if you do not have enough space in the /home directory. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for more information.) See the *IBM Tivoli Directory Server Version 5.2 Server Readme* file and the *IBM Tivoli Directory Server Version 5.2 Readme Addendum* for any last minute changes to database requirements. (See "Accessing publications online" on page viii for information about accessing online publications.)

Other software
- The Korn shell is required.
- HP-UX Runtime Environment for the Java 2 Platform Version 1.4.1. is required for the Configuration Tool and for GSKit. Go to http://www.hp.com/go/java to download Java.
- To use GSKit, Patch PHSS_26946 is required for the gsk runtime.
- Set the current kernel configuration parameters. See "Setting the current kernel configuration parameters" on page 73 for the required parameters.
- DB2 Universal Database for AIX version 8.1 Enterprise Server Edition with FixPak 2 (DB2) is included with the IBM Tivoli Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

Requirements for the Web Administration Tool

You can install the Web Administration Tool on a computer with or without the client or the server. The Web Administration Tool can be used to administer LDAP servers of the following types:

- IBM Tivoli Directory Server 5.2

- IBM Directory Server 5.1
- IBM Directory Server 4.1
- IBM SecureWay Directory 3.2.2
- OS/400 V5R3
- z/OS R4

  Note: For z/OS R4, only the following setups are supported:
  - A single TDBM backend
  - A single SDBM backend
  - One TDBM and SDBM backend

The Web Administration Tool is supported on the following operating system platforms:

Windows platforms:
- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003 Standard, Enterprise

AIX platforms:
AIX 4.3.3, 5.1, or 5.2

xSeries Linux platforms:
- UnitedLinux 1.0
- SuSE Linux Enterprise Server 7 or 8
- Red Hat Advanced Server 2.1
- Red Hat Enterprise Linux 3.0

zSeries Linux platforms:
- Red Hat Advanced Server 3.0
- SuSE Linux Enterprise Server 8.0

iSeries and pSeries Linux platforms:
- UnitedLinux 1.0
- SuSE Linux Enterprise Server 8.0
- Red Hat Advanced Server 3.0

Solaris platforms:
- Solaris 7, 8, or 9

HP-UX platforms:
HPUX 11 or 11i

To use the Web Administration Tool, you also need the following:

- One of the following application servers:
  - The embedded version of WebSphere Application Server - Express V5.0 or later. Version 5.0.2 is Provided with IBM Tivoli Directory Server 5.2. (iSeries Linux, pSeries Linux, and HP-UX require version 5.0.2.) If you have version 5.0, which was provided with IBM Directory Server, installed, see "Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express" on page 43.

  - IBM WebSphere® 5.0 or later. (iSeries Linux, pSeries Linux, and HP-UX require version 5.0.2.)
- One of the following Web browsers on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed):

  On Windows platforms
  Microsoft Internet Explorer version 6.0

  On AIX
  Mozilla 1.3 or 1.4

  On xSeries Linux
  Mozilla 1.3 or 1.4

  On iSeries, pSeries, zSeries Linux
  No browser support is available.

  On Solaris 7, 8, or 9
  Mozilla 1.3 or 1.4

  On HP-UX
  Mozilla 1.3 or 1.4

Secure Sockets Layer (SSL) Global Security Kit (GSKit)

Global Security Kit (GSKit) version 7a is an optional software package that is required only if Secure Sockets Layer (SSL) Security or Transport Layer Security (TLS) is required.

IBM Tivoli Directory Server 5.2 alone does not provide the capability for SSL connections from IBM Tivoli Directory Server clients. You can enable the SSL feature by installing the IBM GSKit 7a package. The GSKit package includes SSL support and associated RSA Data Security, Inc. (4) technology.

OpenSSL is included in GSKit and may be used for cryptographic operations (as per the OpenSSL license requirements).

The IBM Tivoli Directory Server server can work without the GSKit installed. In this case the server accepts only non-secure connections from any Directory client. Similarly, the IBM Tivoli Directory Server client can work without the GSKit installed. Install GSKit on both the server and the client if you want to use secure connections.

See Appendix I, “Setting up GSKit to support CMS key databases”, on page 139 for more information about setting up GSKit after installation.

Chapter 5. Migration from previous releases

Migrating is necessary to preserve any changes that you have made to the schema definitions and to preserve your data and directory server configuration. Use the procedures in this chapter when you are migrating an existing directory server on the same physical computer from a version of SecureWay Directory or IBM Directory Server.

If your installation includes replica servers, read the information in Appendix C, "Migrating replication servers", on page 123 before you start migrating any of your servers.

Note: If you have only a client installed, migration is generally not necessary. However, if you are migrating from a release prior to IBM Directory Server 4.1 and you have Java applications that use the IBM JNDI JAR files, the JAR files will be removed during installation; therefore, save them before you install IBM Tivoli Directory Server 5.2. See step 2 on page 31 for Windows platforms or step 2 on page 35 for all UNIX platforms for information.

Starting with IBM Directory Server 4.1, IBM JNDI is not supported. IBM Directory Server 4.1, 5.1, and 5.1 for Linux iSeries and pSeries, and IBM Tivoli Directory Server 5.2 include the Sun Microsystems JNDI. See the Sun documentation for information about the Sun JNDI. There might be some functional differences between IBM and Sun implementations that require changes to existing JNDI applications. IBM JNDI applications might still run, but for reliable results, begin using the Sun JNDI immediately.

If you are migrating from SecureWay Directory, see one of the following sections:

- For Windows, see "Migration from SecureWay Directory Version 3.2.2 for Windows InstallShield GUI installations" on page 30.
- For AIX, see "Migration from SecureWay Directory Version 3.2.2 for AIX installations" on page 33
- For Solaris and Linux, see "Migration from SecureWay Directory Version 3.2.2 for Solaris and Linux installations" on page 35.

If you are migrating from IBM Directory Server 4.1, 5.1, or 5.1 for Linux iSeries and pSeries, see one of the following sections:

- For Windows, see "Migration from IBM Directory Server version 4.1 or 5.1 for Windows installations" on page 37.
- For AIX, see "Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations" on page 37
- For Solaris, Linux, zSeries Linux, iSeries and pSeries Linux, or HP-UX, see "Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations" on page 42.

The version of SecureWay Directory you are migrating must be 3.2.2 or higher. If you have a SecureWay Directory version that is less than 3.2.2 currently installed, you must upgrade to version 3.2.2 before installing IBM Tivoli Directory Server 5.2. You can download SecureWay Directory version 3.2.2 from the IBM Directory Web page: http://www.ibm.com/software/tivoli/products/directory-server/

© Copyright IBM Corp. 1998, 2003

Attention

In releases before IBM Directory Server 4.1, the LDAP server uses **LDAP** as its Kerberos service name to communicate with its client and the Kerberos KDC. (For example, LDAP/ldaphost.austin.ibm.com, where ldaphost is the hostname of the computer where the LDAP server is located.) For IBM Directory Server 4.1 and 5.1 and IBM Tivoli Directory Server 5.2, a lowercase service name is used (for example, ldap/ldaphost.austin.ibm.com). Because of this change, an IBM Directory Server 4.1 or 5.1, or IBM Tivoli Directory Server 5.2 server might not be able to start after migrating from a 3.2.2 server. This is because the 4.1, 5.1, or 5.2 server is looking for **ldap** in the keytab file in which an **LDAP** service name was located and used by the previous 3.2.2 server. To correct this situation you can do either of the following:

- Generate a keytab file by adding a lowercase LDAP Kerberos service name and start using the new keytab file to communicate.
- Set the environment variable LDAP_KRB_SERVICE_NAME to **LDAP** before starting the server. This environment variable causes the LDAP server to continue using the uppercase LDAP server service name in the keytab file and to communicate with its clients. In the latter case, the environment variable must be set on the client side as well so that the client will continue using the uppercase LDAP service name to communicate with its server.

The audit log and the change log are not migrated. If you want to preserve your audit log and change log settings, record them before proceeding. After you have installed IBM Tivoli Directory Server, you can reset the audit log settings through the Web Administration Tool and the change log settings through the Configuration Tool. Note that there is a new setting for the Audit version, which is set by default to 2. You must set the Audit version to 1 if you want to maintain your previous audit logging capabilities for any applications that parse the audit log. See the *IBM Tivoli Directory Server Administration Guide* for information.

Attention: Run the **db2ldif** application before uninstalling the 3.2.2 version of SecureWay Directory. Do not use the **DB2BACKUP** command.

Reference your current (pre-IBM Tivoli Directory Server 5.2) documentation for instructions for running the **db2ldif** utility. Databases must not be unconfigured or dropped unless they have been backed up using the 3.2.2 version of **db2ldif**. Failure to comply with this results in a complete loss of data.

Migration from SecureWay Directory Version 3.2.2 for Windows InstallShield GUI installations

If you are upgrading from a 3.2.2 version of SecureWay Directory, and you are installing IBM Tivoli Directory Server on a Windows system using the InstallShield GUI, the installation automatically completes some migration for you.

To migrate, use the following procedure:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *installpath*\etc directory to the *installpath*\etc\userV52 directory. (You must create the *installpath*\etc\userV52 directory.) *installpath* is the directory where SecureWay Directory is installed.

These include files with the following file extensions:
- .oc
- .at
- .conf

and the following files:
- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

2. If you have any existing IBM JNDI applications, IBMJNDI.JAR or any associated JNDI files, you can save them if you like, although IBM JNDI is no longer supported. To save the files:
   - Save files, including any subdirectories, in *installpath*\jre\bin to *installpath*\etc\userV52\jre\bin
   - Save files, including any subdirectories, in *installpath*\jre\lib to *installpath*\etc\userV52\jre\lib

   JNDI-related files are:
   - Ibmjcefw.jar
   - Ibmjceprovider.jar
   - IBMjgssprovider.jar
   - Local_policy.jar
   - US_export_policy.jar
   - Krb5.ini
   - Ibmjndi.jar
   - Ibmjndi.zip
3. If you have not done so already:
   a. Export the database using **db2ldif**:
      ```
      db2ldif -o outputfile
      ```

      where *outputfile* specifies the LDIF output file to contain the directory entries in LDIF format.

      For more information about the **db2ldif** command, read the **db2ldif** documentation in the *SecureWay Administration Guide* for your release before exporting the database.

      Attention: Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.
   b. Unconfigure and remove the database by typing the following at a command prompt:
      ```
      ldapucfg -d
      ```
   c. Type `y` to confirm the removal. Default LDAP databases and instances are automatically removed from the system when the command successfully completes. (If your database instance name and your database name are both **ldapdb2**, you have a default database configured.)

      Notes:
      1) If you use a custom database, you must manually remove the DB2 database from the system.

    2) Data contained in the SecureWay Directory 3.2.2 database is not compatible with IBM Tivoli Directory Server 5.2 unless it is exported using the 3.2.2 version of **db2ldif** and imported through the **bulkload** utility provided with IBM Tivoli Directory Server 5.2.
    3) The server will not start if you do not migrate the database.
    4) The changes in the changelog database are not compatible with the new data format and cannot be used. The existing changelog settings contained in the slapd32.conf file will be migrated to the new configuration.
    5) The audit log will not be migrated and must be reconfigured.
    6) If you have a version of DB2 earlier than version 7.2 with FixPak 5, you must upgrade to DB2 7.2 FixPak 5 or later after you have exported the database. Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Tivoli Directory Server.

Installation steps:

4. Install IBM Tivoli Directory Server 5.2 using the InstallShield GUI. See "Installing IBM Tivoli Directory Server on a Windows platform" on page 50 for instructions. The InstallShield GUI automatically migrates the configuration and schema files.

   Notes:

   a. You might be asked if you want to replace some configuration files. Select **Yes** to replace.
   b. If a configured database is detected, you are instructed that additional steps must be taken before the installation can continue. The installation program lists the steps needed to be taken before the installation can continue. The installation program exits after you acknowledge that these steps are required. The IBM Tivoli Directory Server installation program repeats this action as long as there is an existing database configured.

Post-installation steps:

5. After you complete the installation and restart your computer, the Configuration Tool starts automatically. Use the Configuration Tool to set the Administrator DN and password and configure a new LDAP database. See Chapter 12, "Configuration", on page 83 for instructions on how to configure the LDAP database.

   Note: If you want a change log database, make sure the change log is enabled through the Configuration Tool or by using the **ldapcfg** utility with the **-g** option.
6. Use the **bulkload** utility to import the **db2ldif** exported data, as follows:

   ```
   bulkload -i ldiffile -c -d
   ```

   where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory.

   Note: Read the **bulkload** documentation in the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for information about command line settings that provide additional levels of function.

Migration from SecureWay Directory Version 3.2.2 for AIX installations

The instructions in this section are for AIX installations. For Solaris and Linux, see "Migration from SecureWay Directory Version 3.2.2 for Solaris and Linux installations" on page 35.

To migrate an existing directory server on AIX, use the following procedure:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *install path*/etc directory to the *install path*/etc/userV52 directory. (You must create the *install path*/etc/userV52 directory.) *install path* is the directory where SecureWay Directory is installed.

   These include files with the following file extensions:
   - .oc
   - .at
   - .conf

   and the following files:
   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema
2. If you have any existing IBM JNDI applications, IBMJNDI.JAR or any associated JNDI files, you can save them if you like, although IBM JNDI is no longer supported. To save the files:
   - Save files, including any subdirectories, in *installpath*\java\bin to *installpath*\etc\userV52\java\bin
   - Save files, including any subdirectories, in *installpath*\java\lib to *installpath*\etc\userV52\java\lib

   JNDI-related files are:
   - Ibmjcefw.jar
   - Ibmjceprovider.jar
   - IBMjgssprovider.jar
   - Local_policy.jar
   - US_export_policy.jar
   - Krb5.ini
   - Ibmjndi.jar
   - Ibmjndi.zip
3. Export the database using **db2ldif**, as follows:

   ```
   db2ldif -o outputfile
   ```

   where *outputfile* specifies the LDIF output file to contain the directory entries in LDIF format.

   For more information about the **db2ldif** command, read the **db2ldif** documentation in the *SecureWay Administration Guide* for your release before exporting the database.

   Attention: Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.

4. Unconfigure and remove the database by typing the following at a command prompt:

   ```
   ldapucfg -d
   ```

5. Type y to confirm the removal. Default LDAP databases are automatically removed from the system when the command successfully completes. (If your database instance name and your database name are both **ldapdb2**, you have a default database configured.)

   Notes:

   a. If you use a custom database, you must manually remove the DB2 database from the system.
   b. Data contained in the SecureWay Directory 3.2.2 database is not compatible with IBM Tivoli Directory Server 5.2 unless it is exported using **db2ldif** and imported through the **bulkload** utility provided with IBM Tivoli Directory Server 5.2.
   c. The server will not start if you do not migrate the database.
   d. If you have a version of DB2 earlier than version 8.1 with FixPak 2, you must upgrade to DB2 8.1 FixPak 2 after you have exported the database. Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Tivoli Directory Server.
   e. The changes in the change log database are not compatible with the new data format and cannot be used. Any entries in the change log will be lost. The existing change log settings contained in the slapd32.conf file will be migrated to the new configuration.
   f. The audit log will not be migrated and must be reconfigured.

Installation steps:

6. Install IBM Tivoli Directory Server 5.2 using SMIT. For information, see "SMIT installation" on page 58.

Post-installation steps:

7. Migrate the configuration and schema by executing the migrate52 script. Type the following commands at a command prompt:

   ```
   cd installpath/etc
   ../sbin/migrate52
   ```

   Note: You must run the migrate52 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

8. Set the Administrator DN and password and configure a new LDAP database using the **ldapcfg** or **ldapxcfg** commands. See Chapter 12, "Configuration", on page 83 for instructions on how to configure the LDAP database.

   Note: If you want a change log database, make sure the change log is enabled through the Configuration Tool or by using the **ldapcfg** command with the **-g** option.

9. Use the **bulkload** utility to import the **db2ldif** exported data:

   ```
   bulkload -i ldiffile -c -d
   ```

   where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory.

   Note: Read the **bulkload** documentation in the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for command line settings that provide additional levels of function.

Migration from SecureWay Directory Version 3.2.2 for Solaris and Linux installations

The instructions in this section are for Solaris and Linux. Do not use these instructions to migrate on an AIX system. If you are migrating on an AIX system, see "Migration from SecureWay Directory Version 3.2.2 for AIX installations" on page 33.

To migrate an existing directory server, use the following procedure:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf file and any schema files from the *installpath*/etc directory to the *install path*/etc/userV52 directory. (You must create the *installpath*/etc/userV52 directory.) *installpath* is the directory where SecureWay Directory is installed.

   These include files with the following file extensions:

   - .oc
   - .at
   - .conf

   and the following files:

   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema
2. If you have any existing IBM JNDI applications, IBMJNDI.JAR or any associated JNDI files, you can save them if you like, although IBM JNDI is no longer supported. To save the files:
   - Save files, including any subdirectories, in *installpath*\java\bin to *installpath*\etc\userV52\java\bin
   - Save files, including any subdirectories, in *installpath*\java\lib to *installpath*\etc\userV52\java\lib

   JNDI-related files are:

   - Ibmjcefw.jar
   - Ibmjceprovider.jar
   - IBMjgssprovider.jar
   - Local_policy.jar
   - US_export_policy.jar
   - Krb5.ini
   - Ibmjndi.jar
   - Ibmjndi.zip
3. Export the database using **db2ldif**, as follows:

   Note: Read the **db2ldif** documentation in the *SecureWay Administration Guide* for your release before exporting the database.

   ```
   db2ldif -o outputfile
   ```

   where *outputfile* specifies the LDIF output file to contain the directory entries in LDIF format.

Attention: Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.

4. Unconfigure and remove the database by typing the following at a command prompt:
```
ldapucfg -d
```
5. Type y to confirm the removal. Default LDAP databases are automatically removed from the system when the command successfully completes. (If your database instance name and your database name are both **ldapdb2**, you have a default database configured.)

   Notes:

   a. If you use a custom database, you must manually remove the DB2 database from the system.
   b. Data contained in the SecureWay Directory 3.2.2 database is not compatible with IBM Tivoli Directory Server 5.2 unless it is exported using **db2ldif** and imported through the **bulkload** utility provided with IBM Tivoli Directory Server 5.2.
   c. The server will not start if you do not migrate the database.
   d. If you have a version of DB2 earlier than version 7.2 with FixPak 5, you must upgrade to DB2 7.2 FixPak 5 or later after you have exported the database. Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Tivoli Directory Server.
   e. The changes in the changelog database are not compatible with the new data format and cannot be used. The existing changelog settings contained in the slapd32.conf file will be migrated to the new configuration.
   f. The audit log will not be migrated and must be reconfigured.
6. Uninstall SecureWay Directory 3.2.2.

Installation steps:

7. Install IBM Tivoli Directory Server 5.2. Use one of the following:
   - **pkgadd** for Solaris. See "Command line installation using pkgadd" on page 69 for information.
   - **RPM** for Linux. See "Installing IBM Tivoli Directory Server" on page 63 for information.
   - The InstallShield GUI. See "Installing on a UNIX-based platform" on page 53 for information.

Post-installation steps:

8. Migrate the configuration and schema by executing the migrate52 script. Type the following commands at a command prompt:
```
cd installpath/etc
../sbin/migrate52
```
   Note: You must run the migrate52 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.
9. Set the Administrator DN and password and configure a new LDAP database using the **ldapcfg** or **ldapxcfg** commands. See Chapter 12, "Configuration", on page 83 for instructions on how to configure the LDAP database.

Note: If you want a change log database, make sure the change log is enabled through the Configuration Tool or the **ldapcfg** command with the **-g** option.

10. Use the **bulkload** utility to import the **db2ldif** exported data:

```
bulkload -i ldiffile -c -d
```

where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory.

Note: Read the **bulkload** documentation in the *IBM Directory Server Version 5.2 Administration Guide* for command line settings that provide additional levels of function.

Migration from IBM Directory Server version 4.1 or 5.1 for Windows installations

If you are upgrading from the 4.1 or 5.1 version of IBM Directory Server on a Windows system using the InstallShield GUI, migration is automated. The InstallShield GUI backs up the server configuration and schema files before installing the 5.2 version, and it migrates these files to the 5.2 version for you automatically.

Note: If you have the Web Administration Tool installed from IBM Directory Server 5.1, see "Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express" on page 43 for information.

Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations

The instructions in this section are for AIX installations. For Solaris, Linux, zSeries Linux, and HP-UX, see "Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations" on page 42.

Note: If you have the Web Administration Tool installed from IBM Directory Server 5.1, see "Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express" on page 43 for information.

This section is divided into three subsections for the following migration scenarios:

- "Migrating from IBM Directory Server 4.1"
- "Migrating from IBM Directory Server 5.1 with DB2 8.1, 32-bit" on page 38
- "Migrating from IBM Directory Server 5.1 with DB2 7.2" on page 39

Migrating from IBM Directory Server 4.1

To migrate an existing IBM Directory Server 4.1 on AIX, use the following procedure:

Pre-installation steps:

1. Back up the previous versions of the slapd32.conf or ibmslapd.conf and any schema files from the /usr/ldap/etc directory to a directory that is not a subdirectory of /usr/ldap.

   These include files with the following file extensions:

   - .oc

- .at
- .conf

and the following files:
- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

2. If you installed with the InstallShield GUI, uninstall using the InstallShield GUI.

Installation steps:

3. Install IBM Tivoli Directory Server 5.2 using the InstallShield GUI or SMIT. See "Installing on a UNIX-based platform" on page 53 or "SMIT installation" on page 58 for information.

Post-installation steps:

4. Migrate the configuration and schema by executing the migrate52 script. Type the following commands at a command prompt:

```
cd installpath/etc
../sbin/migrate52 -s backuppath
```

where *backuppath* is the path where you backed up the files in step 1 on page 37.

Note: You must run the migrate52 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

Migrating from IBM Directory Server 5.1 with DB2 8.1, 32-bit

To migrate an existing IBM Directory Server 5.1 on AIX, migrating DB2 Workgroup Server Edition 8.1, 32-bit, to DB2 Enterprise Server Edition 8.1, 64-bit, use the following procedure:

Pre-installation steps:

1. Stop the database instance, as follows:
   a. Log in as the DB2 instance owner.
   b. Ensure that there are no applications using any databases owned by this DB2 instance. To get a list of all applications owned by the instance, enter the **db2 list applications** command. You can end a session by entering the **db2 terminate** command. Do not force termination of applications using the **db2 force applications all** command, because some applications might have unexpected behavior when they are terminated using this command. See the *DB2 Command Reference* for detailed information about these commands.
   c. When all applications are terminated, stop all database server processes owned by the DB2 instance by entering the **db2stop** command.
   d. Stop the DB2 license daemon by entering the **db2licm end** command.
   e. Stop all command line processor sessions by entering the **db2 terminate** command in each session that was running the command line processor.
   f. Enter the **db2_kill** command to clean up any remaining DB2 resources.
   g. Log off.
2. Back up the previous versions of the slapd32.conf or ibmslapd.conf and any schema files from the /usr/ldap/etc directory to a directory that is not a subdirectory of /usr/ldap.

   These include files with the following file extensions:

- .oc
- .at
- .conf

and the following files:

- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

3. Unconfigure the currently configured IBM Directory Server database (for example, ldapdb2) without deleting the instance and database. You can use the **ldapucfg -d** command or Configuration Tool.
4. Stop the database instance, using the following procedure:
   a. Log in as the instance owner.
   b. Stop the instance using the **db2istop** command:
      ```
      /usr/opt/db2_08_01/instance/db2istop InstName
      ```
5. If you installed with the InstallShield GUI, uninstall using the InstallShield GUI.

Installation steps:

6. Uninstall DB2 Workgroup Server Edition 8.1.
7. Install DB2 Enterprise Server Edition 8.1.
8. Install IBM Tivoli Directory Server 5.2 using the InstallShield GUI or SMIT. See "Installing on a UNIX-based platform" on page 53 or "SMIT installation" on page 58 for information.

Post-installation steps:

9. Update the IBM Tivoli Directory Server database instance to a 64-bit width, as follows:
   a. Log in as **root**.
   b. Run the **db2iupdt** command as follows:
      ```
      /usr/opt/db2_08_01/instance/db2iupdt -w 64 InstName
      ```
10. Migrate the configuration and schema by executing the migrate52 script. Type the following commands at a command prompt:
    ```
    cd installpath/etc
    ../sbin/migrate52 -s backuppath
    ```
    where *backuppath* is the path where you backed up the files in step 2 on page 38

    Note: You must run the migrate52 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

Migrating from IBM Directory Server 5.1 with DB2 7.2

To migrate an existing IBM Directory Server 5.1 on AIX, migrating DB2 Enterprise Server Edition 7.2, 32-bit, to DB2 Enterprise Server Edition 8.1, 64-bit, use the following procedure:

Pre-installation steps:

1. Migrate the DB2 instance. Before you can migrate a DB2 instance, all applications using any databases owned by the instance must be terminated. To prepare a DB2 instance for migration, use the following procedure:
   a. Log in as the DB2 instance owner.

   b. Be sure that there are no applications using any databases owned by this DB2 instance. To get a list of all applications owned by the instance, use the **db2 list applications** command. You can end a session by entering the **db2 terminate** command. Do not force termination of applications using the **db2 force applications all** command, because some applications might have unexpected behavior when they are terminated using this command. See the *DB2 Command Reference* for detailed information about these commands.
   c. When all applications are complete, stop all database server processes owned by the DB2 instance by entering the **db2stop** command.
   d. Stop the DB2 license daemon by entering the **db2licm end** command.
   e. Stop all command line processor sessions by entering the **db2 terminate** command in each session that was running the command line processor.
   f. Enter the **db2_kill** command to clean up any remaining DB2 resources.
   g. Log off.
2. Verify that the database can be migrated. There are also migration considerations you should take into account if you are using the Version 2 user exit program.

   DB2 provides the **db2ckmig** migration command, which is used to verify whether all cataloged databases can be migrated. The **db2imigr** command uses the **db2ckmig** command to verify whether the cataloged databases can be migrated.

   To ensure that you can migrate the instance, run the **db2ckmig** command. If instance migration failed, you must correct the errors reported by this command. You can run the db2ckmig command again to verify that the errors have been corrected, and then migrate the instance.

   For detailed information about the **db2ckmig** command, refer to the *DB2 Command Reference.*

   To verify that all cataloged databases can be migrated, perform the following steps:
   a. Log in as the instance owner.
   b. Enter the following command:
      ```
      DB2DIR/bin/db2ckmig -h -a 0 -l INSTHOME/migration.log
      ```
      where *DB2DIR* = /usr/lpp/db2_06_01
   c. Check the log file. The log file displays the errors that occur when you run the **db2ckmig** command. If it shows any errors, perform corrective actions.
   d. Check that the migration log file is empty before continuing with the instance migration.
   e. Back up the database after making corrections.
3. Install DB2 Enterprise Server Edition 8.1, 64-bit.
4. Back up the previous versions of the slapd32.conf or ibmslapd.conf and any schema files from the /usr/ldap/etc directory to a directory that is not a subdirectory of /usr/ldap.

   These include files with the following file extensions:
   - .oc
   - .at
   - .conf

   and the following files:
   - V3.ldapsyntaxes

- V3.matchingrules
- V3.modifiedschema

5. If you installed with the InstallShield GUI, uninstall using the InstallShield GUI.
6. Migrate the DB2 instance. Only local cataloged databases that reside in the DB2 instance are checked for migration. Uncataloged databases might be unusable after the instance has been migrated.

   After an instance is ready for migration, use the **db2imigr** command to migrate the instance as follows:

   a. Log in as a user with root authority.
   b. If the library_path environment variable is set to /usr/lib and there is a link in /usr/lib to the Version 7 libdb2 shared library, this can cause an error when using the **db2imigr** command. To fix the error, reset the library_path environment variable so that it does not reference the libraries in those paths by entering the following command:

      ```
      unset LIBPATH
      ```

   c. Run the **db2imigr** command as follows:

      ```
      /usr/opt/db2_08_01/instance/db2imigr [-d] [-a AuthType]
               [-u fencedID] InstName
      ```

      where

      - **-d** sets the debug mode that you can use for problem determination. This parameter is optional.
      - **-a** *AuthType* specifies the authentication type for the instance. Valid authentication types are (SERVER), (CLIENT), and (DCS). If the **-a** parameter is not specified, the authentication type defaults to (SERVER), if a DB2 server is installed. Otherwise, the AuthType is set to (CLIENT). This parameter is optional.

        Notes:

        1) The authentication type of the instance applies to all databases owned by the instance.
        2) While authentication type (DCE) is an optional parameter, it is not valid to choose (DCE) for this command
      - **-u** *fencedID* is the user under which the fenced user-defined functions (UDFs) and stored procedures will execute. This parameter is optional only when a DB2 Run-Time Client is installed. It is required for all other DB2 products.
      - *InstName* is the login name of the instance owner.
7. Convert the DB2 instance to a 64-bit width, using the following procedure:
   a. Log in as a user with root authority.
   b. Run the **db2iupdt** command as follows:

      ```
      /usr/opt/db2_08_01/instance/db2iupdt -w 64 InstName
      ```

   c. After migrating the DB2 instance, reset LIBPATH to its original setting
8. Migrate the database owned by the instance, using the following steps:
   a. Log on with a user ID that has SYSADM authority, such as the instance owner.
   b. Ensure that the database you want to migrate is cataloged.
   c. Run **db2**.
   d. At the DB2 command prompt, type the following:

```
migrate database DATABASE-NAME
```

9. Initialize the database manager configuration parameter UTIL_IMPACT_LIM to its default value. The UTIL_IMPACT_LIM configuration parameter did not exist for UDB 7.1 and on migration to Enterprise Server Edition 8.1 it is assigned a value of 0. The valid range for this parameter is 1 to 100. Use the following procedure:
    a. Log on with a user ID that has SYSADM authority.
    b. Run **db2**.
    c. At the DB2 command prompt, type the following:
    ```
    update database manager configuration using UTIL_IMPACT_LIM value
    ```
    value should be kept low: between 1 and 10.

Installation steps:

10. Install IBM Tivoli Directory Server 5.2 using the InstallShield GUI or SMIT. See "Installing on a UNIX-based platform" on page 53 or "SMIT installation" on page 58 for information.

Post-installation steps:

11. Migrate the configuration and schema by executing the migrate52 script. Type the following commands at a command prompt:
    ```
    cd installpath/etc
    ../sbin/migrate52 -s backuppath
    ```
    where *backuppath* is the path where you backed up the files in step 4 on page 40.

    Note: You must run the migrate52 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations

The instructions in this section are for Solaris, Linux, zSeries Linux, iSeries and pSeries Linux, and HP-UX. Do not use these instructions to migrate on an AIX system. If you are migrating on an AIX system, see "Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations" on page 37.

Note: If you have the Web Administration Tool installed from IBM Directory Server 5.1, see "Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express" on page 43 for information.

To migrate an existing directory server, use the following procedure:

Pre-installation steps:

1. Back up the previous versions of the slapd32.conf or ibmslapd.conf and any schema files from the *installpath*/etc directory to the *installpath*/etc/userV52 directory. (You must create the *installpath*/etc/userV52 directory.) *installpath* is the directory where IBM Directory Server 4.1 or 5.1 is installed.

    These include files with the following file extensions:
    - .oc
    - .at
    - .conf

and the following files:

- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

2. Uninstall IBM Directory Server 4.1 or 5.1, using the same utility you used to install. (Do **not** uninstall on HP-UX.)

Installation steps:

3. Install IBM Tivoli Directory Server 5.2 using one of the following:
   - **pkgadd** for Solaris. See "Command line installation using pkgadd" on page 69 for information.
   - **RPM** for Linux. See "Installing IBM Tivoli Directory Server" on page 63 for information.
   - **swinstall** for HP-UX. See Chapter 10, "Installing IBM Tivoli Directory Server using HP-UX utilities", on page 73 for information.
   - InstallShield GUI. See "Installing on a UNIX-based platform" on page 53 for information.
4. Migrate the configuration and schema by executing the migrate52 script. Type the following commands at a command prompt:

   ```
   cd installpath/etc
   ../sbin/migrate52
   ```

   Note: You must run the migrate52 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express

If you currently have the Web Administration Tool from IBM Directory Server 5.1 installed into the embedded version of WebSphere Application Server - Express V5.0, you can use one of the following sections to install the 5.0.2 fix pack for the embedded version of WebSphere Application Server - Express V5.0 and migrate to the 5.2 Web Administration Tool.

For Windows installations

On Windows installations, if you use the InstallShield GUI to install, the embedded version of WebSphere Application Server - Express V5.0 is upgraded to 5.0.2 during installation, and the Web Administration Tool is installed into the embedded version of WebSphere Application Server - Express. This is the preferred method of installation for Windows. The following section is provided for reference.

On Windows, it is possible to upgrade the embedded version of WebSphere Application Server - Express V5.0 and migrate the Web Administration Tool as follows:

1. Download fix pack 2 for the embedded version of WebSphere Application Server - Express V5.0 from the Web site where you downloaded IBM Tivoli Directory Server.
2. Back up the following configuration files, which are in the `WASPath\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\` directory:
   - security\console_passwd

- IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
- IDSConfig\IDSServersConfig\IDSServersInfo.xml

where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express V5.0 that was provided with IBM Directory Server V5.1. If you used the recommended path, *WASPath* is *ldaphome*\appsrv\.

3. Run the following command to uninstall the Web Administration Tool:

```
WASPath\bin\wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
```

4. Install the 5.0.2 fix pack for the embedded version of WebSphere Application Server - Express as follows:
   a. Stop the application server if it is running, using the command:

   ```
   WASPath\bin\stopServer.bat server1
   ```

   b. Install the fix pack by typing the following commands:

   ```
   set JAVA_HOME=WASPath\java
   WAS_FP2_Path\updateSilent.sh -installDir \WASPath -fixpack -install
     -fixpackDir \WAS_FP2_Path\fixpacks -skipIHS -skipMQ
     -fixpackID was50_express_fp2_win -noBackup -noLog -noHistory
   ```

   where *WAS_FP2_Path* is the directory where you downloaded the fix pack in step 1 on page 43.
5. Install the Web Administration Tool provided with IBM Tivoli Directory Server 5.2 if you have not done so already.
6. Install the new Web Administration Tool into the embedded version of WebSphere Application Server - Express V5.0.2, using the instructions in "Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express" on page 125.
7. Restore the Web Administration Tool configuration files that you backed up in step 2 on page 43.
8. Start the embedded version of WebSphere Application Server - Express. See "Starting the application server to use the Web Administration Tool" on page 97.

Note: If you plan to use the Web Administration Tool in a non-English language, see "Corruption of data entered in Web Administration Tool" on page 111.

For UNIX installations

On UNIX installations other than zSeries Linux, migrate the Web Administration Tool as follows:

1. Download fix pack 2 for the embedded version of WebSphere Application Server - Express V5.0 from the Web site where you downloaded IBM Tivoli Directory Server.
2. Back up the following configuration files, which are in the `WASPath/installedApps/DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/` directory:
   - security/console_passwd
   - IDSConfig/IDSSessionConfig/IDSSessionMgmt.xml
   - IDSConfig/IDSServersConfig/IDSServersInfo.xml

   where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express V5.0 that was provided with IBM Directory Server V5.1. If you used the recommended path, *WASPath* is *ldaphome*/appsrv/.

3. Run the following command to uninstall the Web Administration Tool:

   ```
   WASPath/bin/wsadmin.sh -conntype NONE -c "\$AdminApp uninstall IDSWebApp.war"
   ```

4. Install the 5.0.2 fix pack for the embedded version of WebSphere Application Server - Express as follows:

   a. Stop the application server if it is running, using the command:

      ```
      WASPath/bin/stopServer.sh server1
      ```

   b. Install the fix pack by typing the following commands:

      ```
      export JAVA_HOME=WASPath/java
      WAS_FP2_Path/updateSilent.sh -installDir /WASPath -fixpack -install
        -fixpackDir /WAS_FP2_Path/fixpacks -skipIHS -skipMQ
        -fixpackID fp_name -noBackup -noLog -noHistory
      ```

      where

      - *WAS_FP2_Path* is the directory where you downloaded the fix pack in step 1 on page 44.
      - *fp_name* is the name of the fix pack and depends on the operating system platform:

        AIX was50_express_fp2_aix

        xSeries Linux
        was50_express_fp2_linux

        Solaris
        was50_express_fp2_solaris

        HP-UX
        was50_express_fp2_hpux

5. Install the Web Administration Tool provided with IBM Tivoli Directory Server 5.2 if you have not done so already.
6. Install the new Web Administration Tool into the embedded version of WebSphere Application Server - Express V5.0.2, using the instructions in "Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express" on page 125.
7. Restore the Web Administration Tool configuration files that you backed up in step 2 on page 44.
8. Start the embedded version of WebSphere Application Server - Express. See "Starting the application server to use the Web Administration Tool" on page 97.

Note: If you plan to use the Web Administration Tool in a non-English language, see "Corruption of data entered in Web Administration Tool" on page 111.

For zSeries Linux installations

To upgrade the embedded version of WebSphere Application Server - Express on zSeries Linux:

1. In the *WAS_home*/bin directory, run the following command to create a backup of your existing configuration:

   ```
   backupConfig.sh
   ```

   This creates a zip file called WebSphereConfig_*yyyy-mm-dd*.zip.
2. Move this zip file to a directory outside your *WAS_home* directory.

WAS_home is the directory where the embedded version of WebSphere Application Server - Express is installed. This is *ldaphome*/appsrv if you used the recommended directory for installation.

3. Back up the following configuration files, which are in the `WASPath/installedApps/DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/` directory:
   - security/console_passwd
   - IDSConfig/IDSSessionConfig/IDSSessionMgmt.xml
   - IDSConfig/IDSServersConfig/IDSServersInfo.xml

   where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express V5.0 that was provided with IBM Directory Server V5.1. If you used the recommended path, *WASPath* is *ldaphome*/appsrv/.
4. Uninstall the embedded version of WebSphere Application Server - Express version 5.0 by removing the *WAS_home* directory.
5. Install the embedded version of WebSphere Application Server - Express version 5.0.2
6. In the *WAS_home*/bin directory, run the following command:

   ```
   restoreConfig.sh backup_path/WebSphereConfig_yyyy-mm-dd.zip
   ```

   where *backup_path* is the path where you moved the *WAS_home*/bin/restoreConfig.sh WebSphereConfig_*yyyy-mm-dd*.zip file.

   This command does the following:
   - Creates a backup of the 5.0.2 configuration. (This will be a directory named *WAS_home*/config.old)
   - Copies the 5.0 configuration into the new 5.0.2 installation (in the config directory).
7. Modify the *WAS_home*/config/cells/DefaultNode/security.xml file to include the following <entry> stanzas:

   ```
   <entries xmi:id="JAASConfigurationEntry_6" alias="wssecurity.IDAssertion">
   <loginModules xmi:id="JAASLoginModule_6"
      moduleClassName="com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy"
      authenticationStrategy="REQUIRED">
   <options xmi:id="Property_8" name="delegate"
      value="com.ibm.wsspi.wssecurity.auth.module.IDAssertionLoginModule"/>
   </loginModules>
   </entries>
   <entries xmi:id="JAASConfigurationEntry_7" alias="wssecurity.Signature">
   <loginModules xmi:id="JAASLoginModule_7"
      moduleClassName="com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy"
      authenticationStrategy="REQUIRED">
   <options xmi:id="Property_9" name="delegate"
      value="com.ibm.wsspi.wssecurity.auth.module.SignatureLoginModule"/>
   </loginModules>
   </entries>
   ```

   Note: Some lines have been broken in the example to fit on the page. Be sure to enter each of the `loginmodules` entries and each of the `options` entries on a single line.

   If you added entries in the 5.0 configuration before performing this manual migration, you might have to change the IDs for the entries.
8. At the server level, copy all occurrences of the ws-security.xml file from the *WAS_home*/config.old directory into the corresponding location in the *WAS_home*/config directory.

9. At the server level of the templates directory, copy the variables.xml and ws-security.xml files from the *WAS_home*/config.old directory into the corresponding location in the *WAS_home*/config directory.
10. Copy the server.xml file from the *WAS_home*/config.old/templates/system/nodes/servers/jmsserver into the corresponding location in the *WAS_home*/config directory.
11. Copy the *WAS_home*/config.old/templates/system/jdbc-resource-provider-templates.xml file into the corresponding location in the *WAS_home*/config directory.
12. Run the following command to uninstall the Web Administration Tool:

    ```
    WASPath/bin/wsadmin.sh -conntype NONE -c "\$AdminApp uninstall IDSWebApp.war"
    ```
13. Install the Web Administration Tool provided with IBM Tivoli Directory Server 5.2 if you have not done so already. See Chapter 8, "Installing IBM Tivoli Directory Server using Linux utilities", on page 63.
14. Install the new Web Administration Tool into the embedded version of WebSphere Application Server - Express V5.0.2, using the instructions in "Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express" on page 125.
15. Restore the Web Administration Tool configuration files that you backed up in step 3 on page 46.
16. Start the embedded version of WebSphere Application Server - Express. See "Starting the application server to use the Web Administration Tool" on page 97.

Note: If you plan to use the Web Administration Tool in a non-English language, see "Corruption of data entered in Web Administration Tool" on page 111.

Chapter 6. Installing using the InstallShield GUI

You can use the InstallShield GUI to install IBM Tivoli Directory Server on Windows, AIX, and Solaris platforms. It is also available for xSeries Linux platforms. If you do not want to use the InstallShield GUI to install, this guide contains a manual installation procedure for each platform in separate chapters. For an example, see Chapter 7, “Installing IBM Tivoli Directory Server using AIX utilities”, on page 57.

Be sure that the requirements for your operating system are met before you begin installation. See Chapter 4, “System requirements”, on page 13 for information.

Attention

See “Migration from SecureWay Directory Version 3.2.2 for AIX installations” on page 33 or “Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations” on page 37 for instructions for migrating and restoring backed-up files after reinstallation on an AIX system.

Read and understand the migration process in “Migration from SecureWay Directory Version 3.2.2 for Solaris and Linux installations” on page 35 or “Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations” on page 42 for instructions for migrating and restoring backed-up files after reinstallation on a Linux, Solaris, or HP-UX system.

If you have SecureWay Directory version 3.1.1.5, 3.2, 3.2.1, or 3.2.2 or IBM Directory Server 4.1 or 5.1 installed on a Windows system, read and understand the migration process in “Migration from SecureWay Directory Version 3.2.2 for Windows InstallShield GUI installations” on page 30 or “Migration from IBM Directory Server version 4.1 or 5.1 for Windows installations” on page 37 before installing IBM Tivoli Directory Server 5.2.

It is very important that you back up and export previous versions of schema files and the server configuration file before installing IBM Tivoli Directory Server 5.2.

If you install IBM Tivoli Directory Server using the InstallShield GUI, you must also uninstall using the InstallShield GUI. This is also true for installation of corequisite products such as DB2, the embedded version of WebSphere Application Server - Express, and GSKit. See “Uninstalling IBM Tivoli Directory Server” on page 100 for instructions for removing IBM Tivoli Directory Server using the InstallShield GUI.

Installing on a Windows platform

Use the information in the following sections to install IBM Tivoli Directory Server 5.2 on a Windows platform using the InstallShield GUI.

Before you install

Before installing, be sure that the following conditions are met. If these conditions are not met, the installation program will exit.

© Copyright IBM Corp. 1998, 2003

- **If you have a version of SecureWay Directory earlier than 3.2.2 installed on your system:**

  Upgrade to 3.2.2 or later before installing IBM Tivoli Directory Server 5.2. Then use the instructions in Chapter 5, "Migration from previous releases", on page 29 to migrate your data and install IBM Tivoli Directory Server 5.2.
- **If you have SecureWay Directory version 3.2.2 or IBM Directory Server 4.1 or 5.1 installed on your computer**:

  Use the instructions in Chapter 5, "Migration from previous releases", on page 29 to migrate your data and install IBM Tivoli Directory Server 5.2.
- **If you have a version of DB2 earlier than 7.2 with FixPak 5 installed on your computer:**

  Upgrade to DB2 7.2 FixPak 5 or later, or remove DB2. DB2 8.1 with FixPak 2 is included with IBM Tivoli Directory Server. If you do not have a version of DB2 on your system, the InstallShield GUI installs it if you choose to install the server.

  Attention: Export your data using **db2ldif** before unconfiguring and removing your current database. Do not use the **DB2BACKUP** command. If you do not export before unconfiguring and removing the database, you will lose your data.
- **If you have the embedded version of WebSphere Application Server - Express installed on your computer:**

  The embedded version of WebSphere Application Server - Express v5.0.2 is provided with IBM Tivoli Directory Server 5.2. If version 5.0 of the embedded version of WebSphere Application Server - Express is already installed, the InstallShield GUI installation program upgrades it to version 5.0.2.

Creating the DB2 database owner

Before you install, create or be sure that you have created the user ID that will own the DB2 database used to store the directory data. You will be asked to provide this user ID and its password during configuration, which runs automatically after installation and system restart. The user ID must be 8 characters or less, and it must be a member of the Administrators group. If you are creating a new database, a DB2 instance with the same name as the user ID will be created to hold the database.

Installing IBM Tivoli Directory Server on a Windows platform

To install IBM Tivoli Directory Server 5.2:

1. On the computer where you are installing the IBM Tivoli Directory Server, stop any programs that are running and close all windows. If you have open windows, the initial IBM Tivoli Directory Server installation window might be hidden behind other windows.
2. If you are installing from a CD, insert the CD in your CD-ROM drive.
3. If you are installing locally from a CD or remotely from the network, go to the drive for your CD-ROM or for the appropriate network path. If you downloaded a zipped file, go to the directory where you unzipped the file.
4. In the \ismp folder, double-click the **setup.exe** icon.

   The language window is displayed.

   Note: When installing on Windows, if the installation program exits without displaying the language window, it might be caused by one of the following:

   - Backlevel video drivers. Update your video drivers to the most recent levels to correct this.

        - Not enough space in the directory specified by the TEMP environment variable. Be sure that you have at least 100 MB of free space in this directory.

5. Select the language you want to use during IBM Tivoli Directory Server installation. Click **OK**.

   Note: This is the language used in the installation program, not in IBM Tivoli Directory Server. You choose the language used in IBM Tivoli Directory Server in step 11.
6. On the Welcome window, click **Next**.
7. If a previous or current version of IBM Tivoli Directory Server is not installed on your system, go to step 8. If a previous version of IBM Tivoli Directory Server is installed on your system, do one of the following:
   - **If you have the server installed on your system from a previous version of IBM Tivoli Directory Server:** You are asked if you want to migrate your configuration. Click **Yes** to migrate or **No** to overwrite your previous installation. See Chapter 5, “Migration from previous releases”, on page 29 for complete migration instructions.

     Attention: If you choose to click **No** and overwrite your previous installation, you will lose your data and any configuration or schema changes you have made will be lost.
   - **If you have the Client SDK installed on your system from a previous version of IBM Tivoli Directory Server:** You are asked if you want to continue with the installation. Click **Yes** to install over the previous version of the Client SDK, or click **No** to exit the installation.
   - **If you have the Web Administration Tool installed on your system from a previous version of IBM Tivoli Directory Server:** You are asked if you want to continue with the installation. Click **Yes** to install over the previous version of the Web Administration Tool, or click **No** to exit the installation.
   - **If you have the current version of the server, the client SDK, or the Web Administration Tool installed on your system:** You are asked if you want to exit the installation. If you do not exit and back up your files, they will be overwritten during the installation.
   - If you have the 5.0 version of the embedded version of WebSphere Application Server - Express installed, you are told that it will be upgraded to the 5.0.2 version.
8. After reading the Software license agreement, select **I accept the terms in the license agreement**. Click **Next**.
9. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
10. To install to the default directory, click **Next**. You can specify a different directory by clicking **Browse**.

    Note: Do not use special characters, such as hyphen (-) and period (.) in the name of the installation directory. If you do not use the default location, use a name such as **ldap** or **ldapdir**. Do not use a name such as **ldap-dir** or **ldap.dir**.
11. Select the language you want to use in IBM Tivoli Directory Server 5.2. Click **Next**.
12. A window showing the following components for installation is displayed:
    - Client SDK 5.2
    - Web Administration Tool 5.2

- Server 5.2
- IBM WebSphere Application Server - Express 5.0.2
- DB2 V8.1
- GSKit

The components that are not yet installed are preselected. You can choose to reinstall the server, the client, or the Web Administration Tool if they were previously installed.

Notes:

a. If you install the Web Administration Tool, Directory Services Markup Language (DSML) files are also copied to your computer. See Appendix F, "Installing and configuring DSML", on page 131 for information about installing and configuring DSML.

b. If you install the Web Administration Tool, an application server is required to run the tool. If you select **IBM WebSphere Application Server - Express** and you do not have the 5.0 version installed, the embedded version of WebSphere Application Server - Express, v5.0.2 is installed and configured for you. If version 5.0 of the embedded version of WebSphere Application Server - Express is already installed, the InstallShield GUI installation program upgrades it to version 5.0.2. Any configuration files from the previous Web Administration Tool are backed up and restored. If you use another application server, such as WebSphere, you must install the Web Administration Tool file, IDSWebApp.war, into the application server after you install. For information about installing the embedded version of WebSphere Application Server - Express into WebSphere, see Appendix E, "Installing the Web Administration Tool into WebSphere", on page 129.

This window also indicates the amount of disk space required and available on the selected drive.

Be sure the components you want to install are selected, and click **Next**.

13. If you selected **DB2 V8.1** in step 12 on page 51, a window is displayed prompting you to enter a Windows user ID and password for the DB2 system ID. The default user ID is **db2admin**. On the window:
    a. Type the user ID or accept the default.
    b. Type the password, and then type the password again for verification.
    c. Click **Next**.

    Notes:

    a. This user ID must **not** be the one you created in "Creating the DB2 database owner" on page 50.
    b. If you are using an existing Windows user ID, be sure that your password is correct. Otherwise, DB2 does not install correctly.
    c. If you are using an existing Windows user ID, it must be a member of the Administrators group.
    d. If you are not using an existing user ID, DB2 creates the user ID you specify with the password you type.
14. The installation program now has enough information to begin installing. A summary window displays the components you selected and the locations where the selected components will be installed. Click **Back** to change any of your selections. Click **Next** to begin installation.

Note: After installation has begun, do not try to cancel the installation. If you inadvertently cancel the installation, see "Recovering from a failed installation" on page 106 before you attempt to reinstall.

15. After the files are installed:
    - If you installed the client, the Client Readme file is displayed. Read the file and click **Next**.
    - If you installed the server, the server Readme file is also displayed. Read the file and click **Next**.
    - If you installed the Web Administration Tool, the Web Administration Tool Readme file is also displayed. Read the file and click **Next**.
16. Select to restart your computer now or later. Click **Finish**.

    Note: If you installed the server, you must restart your system to complete IBM Tivoli Directory Server configuration. You are unable to use IBM Tivoli Directory Server until this is completed.

After your computer is restarted, if you installed the server, log in using the same user ID that you used to install IBM Tivoli Directory Server. The Configuration Tool automatically runs so that you can complete the server configuration. Before you can use the server, you must set the administrator DN and password and configure the database that will store the directory data. To complete configuration, use the following instructions:

1. To set the administrator DN and password, use the instructions in "Setting the Administrator DN and password" on page 84.
2. To configure the database, use the instructions in "Configuring the database" on page 86.

You have completed installation and configuration.

To make changes to your configuration at a later time, see Chapter 12, "Configuration", on page 83 for more information about using the Configuration Tool.

If any errors occurred during installation or configuration, see Chapter 15, "Troubleshooting", on page 105 for information.

Installing on a UNIX-based platform

Use the information in the following sections to install IBM Tivoli Directory Server 5.2 on a UNIX-based platform using the InstallShield GUI.

Before you install

Before you install, be sure that the following conditions are met:

- **If you have a version of SecureWay Directory installed on your system**, see "Migration from SecureWay Directory Version 3.2.2 for AIX installations" on page 33 or "Migration from SecureWay Directory Version 3.2.2 for Solaris and Linux installations" on page 35.
- **If you have a version of IBM Directory Server installed on your system**, see "Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations" on page 37 or "Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations" on page 42.
- **If you have the embedded version of WebSphere Application Server - Express installed on your computer:**

The embedded version of WebSphere Application Server - Express v5.0.2 is provided with IBM Tivoli Directory Server 5.2. If version 5.0 of the embedded version of WebSphere Application Server - Express is already installed, use the instructions in "Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express" on page 43 to install fix pack 2 for the embedded version of WebSphere Application Server - Express and to upgrade the Web Administration Tool.

Note: Upgrading to version 5.0.2 is not done through the InstallShield GUI on UNIX platforms. You **must** either uninstall the 5.0 version and install 5.0.2 through the InstallShield GUI or follow the manual instructions in "Migrating the Web Administration Tool and upgrading the embedded version of WebSphere Application Server - Express" on page 43.

Installing IBM Tivoli Directory Server on a UNIX-based platform

To install IBM Tivoli Directory Server 5.2:

1. If you are installing from a CD, insert the CD in the CD-ROM drive and mount the CD. If you downloaded a tar file, go to the directory where you untarred the file.
2. From the root directory on the CD or the directory where you untarred the file, type `./setup`. A language window is displayed.
3. Select the language you want to use during IBM Tivoli Directory Server installation. Click **OK**.

   Note: This is the language used in the installation program, not in the IBM Tivoli Directory Server. You choose the language used in the IBM Tivoli Directory Server in step 7
4. On the Welcome window, click **Next**.

Attention: If you have a version of SecureWay Directory or IBM Directory Server already installed on your system, a message is displayed telling you that you must remove it before installing. Before you uninstall, see Chapter 5, "Migration from previous releases", on page 29 for instructions for saving and backing up your data. **If you do not save and back up your data, you will lose it during the uninstallation procedure**.

5. After reading the Software license, select **I accept the terms in the license agreement**. Click **Next**.
6. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
7. Select the language you want to use in IBM Tivoli Directory Server 5.2. Click **Next**.
8. A window is displayed with the following components:
   - Client SDK 5.2
   - Web Administration Tool 5.2
   - Server 5.2
   - IBM WebSphere Application Server - Express 5.0.2
   - DB2 V8.1
   - GSKit

   The components that are not yet installed are preselected.

This window also indicates the amount of disk space required and available on the selected drive.

Be sure the components you want to install are selected, and click **Next**.

Notes:

a. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, “Installing and configuring DSML”, on page 131 for information about installing and configuring DSML.

b. If you install the Web Administration Tool, an application server is required to run the tool. If you select **IBM WebSphere Application Server - Express** and you do not have the 5.0 version installed, the embedded version of WebSphere Application Server - Express, v5.0.2 is installed and configured for you. If you use another application server or if the embedded version of WebSphere Application Server - Express is already installed, you must, after installation, install the IDSWebApp.war file into the application directory for your application server. For information about installing and configuring the embedded version of WebSphere Application Server - Express manually, see Appendix D, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express”, on page 125.

9. The installation program now has enough information to begin installing. A summary panel displays the components you selected and the locations where the selected components will be installed. Click **Back** to change any of your selections. Click **Next** to begin installation.

   Note: During the installation of the server or client on Solaris, if a non-IBM version of LDAP is found, the files are moved to the /usr/bin/ldapsparc directory.

10. After the files are installed:
    - If you installed the client, the Client Readme file is displayed. Read the file and click **Next**.
    - If you installed the server, the Server Readme file is also displayed. Read the file and click **Next**.
    - If you installed the Web Administration Tool, the Web Administration Tool Readme file is also displayed. Read the file and click **Next**.
11. Click **Finish**. Installation is complete.

If you installed the server, the Configuration Tool automatically runs so that you can complete server configuration. Before you can use the server, you must set the administrator DN and password and configure the database that will store the directory data. To complete configuration, use the following instructions:

1. To set the administrator DN and password, use the instructions in “Setting the Administrator DN and password” on page 84.
2. To configure the database, use the instructions in “Configuring the database” on page 86.

You have completed server configuration.

To make changes to your configuration at a later time, see Chapter 12, “Configuration”, on page 83 for more information about using the Configuration Tool.

If any errors occurred during installation or configuration, see Chapter 15, “Troubleshooting”, on page 105for information.

Chapter 7. Installing IBM Tivoli Directory Server using AIX utilities

You can use either of the following utilities to install IBM Tivoli Directory Server on AIX:

- **SMIT** (This is the preferred installation method.) See "SMIT installation" on page 58 for information.
- **installp**. See "Command line installation using installp" on page 60 for information.

Before you install IBM Tivoli Directory Server, be sure you have DB2 Version 8.1 FixPak 2 installed. You can use the **db2_install** command to install the version of DB2 provided.

If you are installing the Web Administration Tool, you must also install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information.

Attention: Use SMIT (see "SMIT installation" on page 58) to install IBM Tivoli Directory Server if you want to migrate from a 3.2.2 version of SecureWay Directory or IBM Directory Server 4.1 or 5.1. Use the appropriate migration process in Chapter 5, "Migration from previous releases", on page 29 before installing the IBM Tivoli Directory Server. Chapter 5, "Migration from previous releases", on page 29 contains instructions for migrating and restoring backed-up files after reinstallation on an AIX system. It is very important that you back up and export previous versions of schema files and the server configuration file before installing the IBM Tivoli Directory Server 5.2.

Notes:

1. Full client and server versions require an X11 environment. Versions of IBM Tivoli Directory Server client and server with no X11 requirements are available in this release. For a client with no X11 requirements, install the minimal client that provides IBM Tivoli Directory Server Client Runtime (ldap.client.rte) and IBM Tivoli Directory Server Client SDK (ldap.client.adt).

   For a server with no X11 requirements, do not install the IBM Tivoli Directory Server Configuration Tool (**ldapxcfg**). **ldapxcfg** is located in the ldap.server.cfg fileset.
2. You do not need to install security functions if you are not going to use them. You can provide SSL by installing a Global Security Kit (GSKit), which is included with IBM Tivoli Directory Server 5.2.
3. If you are installing IBM Tivoli Directory Server on a node within an RS/6000® SP™ environment, see "Before installing on a node within an RS/6000 SP environment" on page 58 before beginning installation.

For more detailed information about installation procedures and commands for the AIX operating system, see the *AIX Installation Guide* provided with the operating system.

© Copyright IBM Corp. 1998, 2003

Before installing on a node within an RS/6000 SP environment

Note: Use this section **only** if you are installing on a node within an RS/6000 SP environment.

If you are installing IBM Tivoli Directory Server on a node within an RS/6000 SP environment you must first add the necessary users and groups to the Control Workstation (CWS) and propagate them out to the nodes using the `/var/sysamn/supper update` command, as follows:

1. Add the **ldap** user and group on the CWS. For example:
   ```
   mkgroup id=300 ldap
   mkuser id=300 ldap
   chgrpmem -m + ldap ldap
   ```
   Note: The user IDs and group IDs used are for the purpose of this example. You can choose different user IDs and group IDs for your environment or use the system defaults.
2. Remove the home directory of the **ldap** user.
   ```
   rm -rf /home/ldap
   ```
3. Update the RS/6000 SP nodes with the new users and groups.
   ```
   /var/sysamn/supper update
   ```

You are now ready to install and configure IBM Tivoli Directory Server on the RS/6000 SP node.

SMIT installation

To install IBM Tivoli Directory Server using **SMIT**:

1. Log in as **root**.
2. Insert the CD containing IBM Tivoli Directory Server 5.2 into the CD-ROM drive and mount the CD, or go to the directory where you untarred the file.
3. At the command prompt, type the following:
   ```
   smit install
   ```
   and press Enter. The Software Installation and Maintenance window is displayed.
4. Click **Install and Update Software**. The Install and Update Software window is displayed.
5. Click **Install and Update from ALL Available Software**.
6. Click **List** next to the **INPUT device/directory for software** field.
7. Select the appropriate CD-ROM drive or the directory containing the IBM Tivoli Directory Server images.
8. Move your cursor to **Software to install**. Do one of the following:
   - Type `ldap` to install all the ldap filesets (or ldap.server, or ldap.client, if appropriate).
   - Click **List** to list all the filesets on the CD, and then select the filesets that you want to install, including different translations of IBM Tivoli Directory Server messages.

     Note: By default **SMIT** installs translated messages based on the language you configured into your AIX system.

If you select the list option, you see, for example:

```
> ldap.client                                                  ALL
     5.2.0.0  Directory Client Runtime (No SSL)
     5.2.0.0  Directory Client SDK


> ldap.html.en_US                                               ALL
     5.2.0.0  Directory HTML Install/Config Gd-U.S. English
     5.2.0.0  Directory HTML Man Pages - U.S. English

> ldap.server                                                   ALL
     5.2.0.0  Directory Server Config
     5.2.0.0  Directory Server Framework (No SSL)
     5.2.0.0  Directory Server Java
     5.2.0.0  Directory Server Runtime

> ldap.webadmin                                                 ALL
     5.2.0.0  Directory Administrative Interface
```

Note: The ldap.html packages are language specific. The ldap.html.en_US package is used as an example.

Select the filesets you want to install and click **OK**.

9. Click **OK**. The message `Are You Sure?` is displayed.
10. Click **OK** to start the installation.
11. Check the installation summary at the end of the output to verify successful installation of the filesets.
12. Click **Done**.
13. To exit **SMIT**, press F12, or click **Cancel** until you are back to a command prompt. To verify that the IBM Tivoli Directory Server was installed successfully, type the following at a command prompt:

    ```
    lslpp -L | grep ldap
    ```

    The output displayed lists all the filesets starting with `ldap`. This list includes the server, client, HTML, and message filesets. For example:

    ```
    ldap.client.adt          5.2.0.0  C  Directory SDK
    ldap.client.rte          5.2.0.0  C  Directory Client
    ldap.html.en_US.config   5.2.0.0  C  Directory HTML
    ldap.html.en_US.man      5.2.0.0  C  Directory HTML man
    ldap.msg.en_US           5.2.0.0  C  Directory Messages
    ldap.server.cfg          5.2.0.0  C  Directory Server
    ldap.server.java         5.2.0.0  C  Directory Server
    ldap.server.com          5.2.0.0  C  Directory Server
    ldap.server.rte          5.2.0.0  C  Directory Server
    ldap.webadmin            5.2.0.0  C  Directory Administrative
    ```
14. If you want to include security functions, install GSKit 7a. See "Installing GSKit" on page 61.

Notes:

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, "Installing and configuring DSML", on page 131 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information about installing and configuring an application server.

Command line installation using installp

Note: If you want to migrate from a 3.2.x version of SecureWay Directory or a version of IBM Directory Server, use the instructions in "SMIT installation" on page 58 to install IBM Tivoli Directory Server.

To install the IBM Tivoli Directory Server from a command prompt:

1. Log on as **root**.
2. Insert the CD containing IBM Directory Version 5.2 into the CD-ROM drive and mount the CD, or go to the directory where you untarred the file.
3. Determine which IBM Tivoli Directory Server packages you need. The packages are as follows:
   - For the server and client, the package name is ldap.server.
   - For the client only, the package name is ldap.client.
   - For the Web Administration Tool, the package name is ldap.webadmin.
   - For all packages, including all language translations of the message files and documentation, the package name is ldap.
4. Determine which language versions of the message files and documentation you need. To see the language versions that are available, type the following command:

   ```
   installp -ld /dev/cd0 | grep ldap
   ```

   A list of all the installable IBM Tivoli Directory Server packages is displayed.

   Some examples of United States English-specific packages are:

   ```
   ldap.html.en_US.man
   ldap.msg.en_US
   ```
5. At the command prompt, install the required packages by typing the following command:

   ```
   installp -acgXd /dev/cd0 packages
   ```

   where :
   - **-a** stands for **apply**.
   - **-c** stands for **commit**.
   - **-g** installs prerequisites if necessary.
   - **-X** increases the file system space if needed.
   - **-d** stands for **device**.
   - *packages* is the package name or list of package names you want to install.

   Examples:

   To install only the IBM Tivoli Directory Server server and client files, type:

   ```
   installp -acgXd /dev/cd0 ldap.server
   ```

   To install all of the IBM Tivoli Directory Server filesets (including messages in every available language), type:

   ```
   installp -acgXd /dev/cd0 ldap
   ```
6. Upon completion of installation, the system generates an installation summary. Verify that the Result column shows **success** for all loaded files. You can also verify that the IBM Tivoli Directory Server was installed successfully by typing the following at a command prompt:

```
lslpp -L | grep ldap
```

The output displayed lists all the filesets starting with `ldap`. This list includes the server, client, Web Administration Tool, HTML, and message filesets. For example:

```
ldap.client.adt        5.2.0.0  C  F   Directory SDK
ldap.client.rte        5.2.0.0  C  F   Directory Client Runtime
ldap.server.cfg        5.2.0.0  C  F   Directory Server Config GUI
ldap.server.com        5.2.0.0  C  F   Directory Server Framework
ldap.server.java       5.2.0.0  C  F   Directory Server Java
ldap.server.rte        5.2.0.0  C  F   Directory Server Runtime
ldap.webadmin          5.2.0.0  C  F   Directory Administrative
```

7. If you want to include security functions, install GSKit 7a. See "Installing GSKit"

Notes:

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, "Installing and configuring DSML", on page 131 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information about installing and configuring an application server.

Installing GSKit

If you installed an SSL-enabled version of IBM Tivoli Directory Server, you must install GSKit to take advantage of the security features. You can use either SMIT or **installp**.

To install using SMIT:

1. Invoke SMIT by typing `smit` at the command line.
2. Select **Software Installation & Maintenance**.
3. Select **Install and Update Software**.
4. Select **Install and Update from ALL Available Software**.
5. On the device/directory window specify the directory that contains the installable software.
6. Select **Package gskta** and **Package gsksa** from the multi-select list.
7. Select the filesets of the software packages to install
8. Select the options appropriate to your installation requirements from the Options window.

   Note: Set the **Install all prereqs** option to **yes**.
9. Confirm that you want to complete the installation.

The **installp** command installs available software products in a compatible installation package. To install GSKit using **installp**, enter the following at a command prompt:

```
installp -acgXd gskta.rte
installp -acgXd gsksa.rte
```

where

- **-a** stands for **apply**

- **-c** stands for **commit**
- **-g** automatically installs or commits any requisite software product.
- **-X** expands the filesystem if necessary.
- **-d** stands for **device**. This specifies where the installation media can be found.

See Appendix I, "Setting up GSKit to support CMS key databases", on page 139 for more information about setting up GSKit after installation.

Setting system variables for AIX operating systems

The ikeyman GUI sets up its own environment except for JAVA_HOME. To see how ikeyman sets its environment, edit the /usr/opt/ibm/gsksa/bin/gsk7ikm-64 file.

You must set the following AIX variable so that ikeyman can run: **JAVA_HOME=***location*, where *location* is the location where JDK 1.3.1 or 1.4.1 is installed.

Note: If you are prompted to set JAVA_HOME, you can set it to either the system-installed Java or the Java version included with the IBM Directory Server. If you use the IBM Directory Server version, you also need to set the LIBPATH environment variable as follows:

```
export LIBPATH=/usr/ldap/java/bin:/usr/ldap/java/bin/classic:$LIBPATH
```

Removing GSKit

To remove GSKit using SMIT:

1. Invoke SMIT by typing `smit` at the command line.
2. Select **Software Installation and Maintenance** on the menu.
3. Select **Software Maintenance and Utilities**.
4. On the Maintenance window, select **Remove Installed Software** to open the Remove Software Product window.
5. Enter the name of the software package
6. Set the flag for **REMOVE dependent software?** to **YES** to instruct the system to automatically remove software products and updates that are dependent upon the product you are removing.
7. Confirm the procedure to complete the removal of the software package.

To remove GSKit using **installp**, type the following at a command prompt:

```
installp -u -g -V2 gskta.rte
installp -u -g -V2 gsksa.rte
```

where

- **-u** removes the specified software and any of its installed updates from the system.
- **-g** removes or rejects dependents of the specified software.
- **-V2** prints an alphabetically ordered list of FAILURES and WARNINGS.

Chapter 8. Installing IBM Tivoli Directory Server using Linux utilities

The instructions in this chapter assume that you are logged in as **root** and have the IBM Tivoli Directory Server Version 5.2 CD mounted at /SD_CDROM.

Attention: If you have SecureWay Directory version 3.1.1.5, 3.2,. 3.2.1, or 3.2.2, or a version of IBM Directory Server installed, and you want to migrate your data, use the instructions in Chapter 5, "Migration from previous releases", on page 29 to install IBM Tivoli Directory Server 5.2. It is very important that you back up and export previous versions of schema files and the slapd32.conf file before installing IBM Tivoli Directory Server 5.2.

Installing IBM Tivoli Directory Server

Note: Before installing IBM Tivoli Directory Server, you must remove any existing versions of LDAP that might have been installed previously. If you try to install IBM Tivoli Directory Server over an existing version of LDAP, IBM Tivoli Directory Server does not install correctly. If this occurs you must remove the IBM Tivoli Directory Server and then reinstall it. See "Uninstalling IBM Tivoli Directory Server" on page 100.

A version of LDAP is installed by default with some operating systems. One method to determine if you have a previously installed version of LDAP is to issue the following command to query the installed packages:

```
rpm -qa | grep -i ldap
```

This command finds any installed applications containing the name ldap. This method works only if you have a version of LDAP that contains the string "ldap" in its application names.

Before you install IBM Tivoli Directory Server, be sure you have DB2 Version 7.2 FixPak 5 or later installed. You can use the **db2_install** command to install the version of DB2 (8.1 FixPak 2) provided.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information.

The IBM Tivoli Directory Server for the Linux operating system is provided in the following packages.

xSeries Linux packages:

- ldap-serverd-5.2-1.i386.rpm
- ldap-clientd-5.2-1.i386.rpm
- ldap-msg-*xxx*-5.2-1.i386.rpm (Where *xxx* is the language identifier.)
- ldap-html-*xxx*-5.2-1.i386.rpm (Where *xxx* is the language identifier.)
- ldap-webadmind-5.2-1.i386.rpm

zSeries Linux packages:

© Copyright IBM Corp. 1998, 2003

- ldap-serverd-5.2-1.s390.rpm
- ldap-clientd-5.2-1.s390.rpm
- ldap-msg-*xxx*-5.2-1.s390.rpm (Where *xxx* is the language identifier.)
- ldap-html-*xxx*-5.2-1.s390.rpm (where *xxx* is the language identifier.)
- ldap-webadmind-5.2-1.s390.rpm

iSeries and pSeries Linux packages:

- ldap-server-5.2-1.ppc.rpm
- ldap-client-5.2-1.ppc.rpm
- ldap-msg-*xxx*-5.2-1.ppc.rpm (where *xxx* is the language identifier.)
- ldap-html-*xxx*-5.2-1.ppc.rpm (where *xxx* is the language identifier.)
- ldap-webadmind-5.2-1.ppc.rpm

Note: The examples in this chapter use Linux Intel-based packages.

To install IBM Tivoli Directory Server:

1. Install the client by typing the following at a command prompt:
   ```
   rpm -ihv ldap-clientd-5.2-1.i386.rpm
   ```
2. Install the server by typing the following at a command prompt:
   ```
   rpm -ihv ldap-serverd-5.2-1.i386.rpm
   ```
3. Verify that the packages have been installed correctly by typing the following at a command prompt:
   ```
   rpm -qa | grep ldap
   ```

   If the product has been successfully installed, the following is displayed:
   ```
   ldap-clientd-5.2-1
   ldap-serverd-5.2-1
   ```
4. Install the language-dependent messages or documents by typing the following at a command prompt:
   ```
   rpm -ihv ldap-msg-xxx-5.2-1.i386.rpm
   rpm -ihv ldap-html-xxx-5.2-1.i386.rpm
   ```
5. If you want to include security functions, install GSKit 7a. See "Installing GSKit" on page 65.

To install the Web Administration Tool:

1. Type the following at a command prompt:
   ```
   rpm -ihv ldap-webadmind-5.2-1.i386.rpm
   ```

   Notes:

   a. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, "Installing and configuring DSML", on page 131 for information about installing and configuring DSML.

   b. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information about installing and configuring an application server.

Installing GSKit

The following information is provided as a guide if you want to install the software package gsk7bas.tar on the Linux operating system. You can install the package through the command line.

The package names for GSKit 7a on the Linux platforms are as follows:

xSeries Linux:
rpm -ihv gsk7bas-7.0-1.0.i386.rpm

zSeries Linux:
gsk7bas-7.0-1.0.s390x.rpm

iSeries and pSeries Linux:
gsk7bas-7.0-1.0.ppc32.rpm

To install GSKit using **rpm**, use one of the following commands:

- To install in the default location, /usr/local, log in as **root** and type the following at a command prompt: (These examples use the xSeries Linux package name.)

  ```
  rpm -ihv gsk7bas-7.0-1.0.i386.rpm
  ```

- To install in a specified location, be sure that you have write access to the directory and use the --noscripts flag, as follows:

  ```
  rpm -ihv --prefix new_locotion gsk7bas-7.0-1.0.i386.rpm --noscripts
  ```

  where *new_location* is the path where you want to install. For example:

  ```
   rpm -ihv --prefix /tmp/usr gsk7bas-7.0-1.0.i386.rpm --noscripts
  ```

See Appendix I, “Setting up GSKit to support CMS key databases”, on page 139 for more information about setting up GSKit after installation.

Removing GSKit

To remove GSKit, type the following at a command prompt:

```
rpm -evv gsk7bas-7.0.1
```

where

- **-evv** specifies to erase the package and display debugging information. If no trace or debug information is desired, use only **-e**.

Chapter 9. Installing IBM Tivoli Directory Server using Solaris utilities

The instructions in this chapter assume that you are logged in as **root** and have the IBM Tivoli Directory Server Version 5.2 CD in the CD-ROM drive.

Attention: If you have a 3.2.x version of SecureWay Directory or a version of IBM Directory Server installed, and you want to migrate your data, use the instructions in Chapter 5, "Migration from previous releases", on page 29 to install IBM Tivoli Directory Server 5.2. It is very important that you back up and export previous versions of schema files and ibmslapd.conf before installing IBM Tivoli Directory Server 5.2.

Installing IBM Tivoli Directory Server

Before you install IBM Tivoli Directory Server, be sure you have DB2 Version 7.2 FixPak 5 or later installed. You can use the **db2_install** command to install the version of DB2 (8.1 FixPak 2) provided.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information.

You can use either the **admintool** utility or **pkgadd** from a command prompt to install IBM Tivoli Directory Server.

Note: You do not need to install security functions if you are not going to use them. You can provide SSL by installing Global Security Kit (GSKit).

The following instructions assume that you are installing from a CD-ROM drive.

Package dependencies

The following IBM Tivoli Directory Server packages are available for installation:

- IBMldapc: IBM Tivoli Directory Server client
- IBMldaps: IBM Tivoli Directory Server server
- IBMldi*xxx*: IBM Tivoli Directory Server documentation (where *xxx* is the language identifier)
- IBMldm*xxx*: IBM Tivoli Directory Server messages (where *xxx* is the language identifier)
- IBMldapw: IBM Tivoli Directory Server Web Administration Tool

Note: The English messages are automatically installed with the IBMldaps (server) package. There is no separate messages package for English.

Because of package dependencies, the order of installation is significant. Install the packages in the following order:

1. Client
2. Server
3. Documentation and Messages

© Copyright IBM Corp. 1998, 2003

If you are installing only the client software, install in the following order:

1. Client
2. Documentation and Messages

If the client package is not installed first, the installation fails.

Note: Because the Web Administration Tool package has no dependencies on any of the other packages, and none of the other packages are dependent on it, you can install it in any order.

"Non-IBM version of LDAP" on your system

During the installation of the server or client on Solaris Operating Environment Software Version 8 or 9, or the server on Version 7, you might encounter the following message:

```
A non-IBM version of LDAP has been located on your system. In order
to use the command line version of the IBM supplied files, the
existing files (ldapadd, ldapdelete, ldaplist, ldapmodify,
ldapmodrdn,  ldapsearch) must be relocated.  Specify the new
directory in which to move the files (/usr/bin/ldapsparc) [?,q]
```

Press Enter to accept the default directory (/usr/bin/ldapsparc), or type a new path name and press Enter, or type `q` and press Enter to quit.

After relocating the files, you might see these additional messages:

```
## Processing system information.
WARNING: /usr/bin/ldapadd <no longer a linked file>
WARNING: /usr/bin/ldapdelete <no longer a linked file>
WARNING: /usr/bin/ldapmodify <no longer a linked file>
WARNING: /usr/bin/ldapmodrdn <no longer a linked file>
WARNING: /usr/bin/ldapsearch <no longer a linked file>
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and
are being used by another package:
/usr/bin/ldapadd
/usr/bin/ldapdelete
/usr/bin/ldapmodify
/usr/bin/ldapmodrdn
/usr/bin/ldapsearch

Do you want to install these conflicting files [y,n,?,q]
```

Type `y` and press Enter to continue the installation. The existing files are moved to the directory previously specified and the IBM Tivoli Directory Server files are installed in the /usr/bin directory.

AdminTool installation

To install IBM Tivoli Directory Server using the **admintool** utility:

1. Type the following at a root command prompt: `admintool&`
   The Users window is displayed.
2. Click **Browse —> Software**. The Software window is displayed.
3. Click **Edit —> Add**. The Set Source Media window is displayed.

Attention: Do not click **Customize** in the lower left corner of the Set Source Media window. If you click **Customize**, the AdminTool installation stops. Because LDAP does not have any customizable options, there is no need for you to click **Customize**.

4. Select **CD with Volume Management**. The CD-ROM path defaults to /cdrom/cdrom0/
5. Change the path to /cdrom/cdrom0/ldap52_us and click **OK**.
6. Click **OK**.
7. Select a package from the following list of installable packages:

   ```
   IBM Tivoli Directory Client
   IBM Tivoli Directory Server
   IBM Tivoli Directory Documentation (for all languages)
   IBM Tivoli Directory Messages (for all languages)
   IBM Tivoli Directory Webadmin
   ```

   Remember that you must install the client package first. See "Package dependencies" on page 67 for the correct installation sequence.
8. Click **Add**.
9. You are asked if you want to use /opt as the base directory. If space permits, use /opt as the base installation directory. To accept /opt as the base directory, press Enter.

   Notes:

   a. With the installation of client and server packages, the system prompts you with the following notice: `This package contains scripts which will be executed with super-user permission during the process of installing the package.` These scripts create the IBM Tivoli Directory Server user ID. Type y to continue.

   b. If you are installing the server package, you will also see the prompt, `Do you want to install these as setuid/setgid files?` Type y to continue.

   After the package is installed, the Software window is displayed.
10. Repeat steps 7 through 9 for each additional package you want to install. When you have finished installing the packages, select **File —> Exit** to exit the **admintool** utility.
11. If you want to include security functions, install GSKit 7a. See "Installing GSKit" on page 71.

Notes:

1. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, "Installing and configuring DSML", on page 131 for information about installing and configuring DSML.
2. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information about installing and configuring an application server.

Command line installation using pkgadd

To install IBM Tivoli Directory Server from a command prompt:

1. Go to the root directory of the directory where you mounted the CD-ROM or where you untarred the tar file.

2. At the command prompt, install the packages you want by typing the following command for each package:

   ```
   pkgadd -d pkgfilename
   ```

   where *pkgfilename* is the file name of the package you want to install. Do not use the system default of **ALL**. The system does not sequence the packages correctly and the installation fails.

   The packages shown in the following table are available. If you are installing the server, you must install the client package first, and then the server package. You can then install the documentation, the messages, and the Web Administration Tool in any order.

Table 1. IBM Directory Server packages for Solaris

Package	**Package name**	**File name**
IBM Tivoli Directory Client	IBMldapc	ldap.client_rted.pkg
IBM Tivoli Directory Server	IBMldaps	ldap.server_rted.pkg
IBM Tivoli Directory documentation	IBMldi*xxx*	ldap.man.*xx_XX*.pkg
IBM Tivoli Directory messages	IBMldm*xxx*	ldap.msg.*xx_XX*.pkg
IBM Tivoli Directory Webadmin	IBMldapw	ldap.webadmin_rted.pkg

xxx and *xx_XX* are specific language identifiers.

Note: The English messages are automatically installed with the IBMldaps (server) package. There is no separate package for English messages.

Examples:

- To install the client package, type:

  ```
  pkgadd -d ldap.client_rted.pkg
  ```

- To install the server package, type:

  ```
  pkgadd -d ldap.server_rted.pkg
  ```

- To install the documentation package, type:

  ```
  pkgadd -d ldap.man.xx_XX.pkg
  ```

- To install the message package, type:

  ```
  pkgadd -d ldap.msg.xx_XX.pkg
  ```

- To install the Web Administration Tool package, type:

  ```
  pkgadd -d ldap.webadmin_rted.pkg
  ```

  Notes:

  a. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, “Installing and configuring DSML”, on page 131 for information about installing and configuring DSML.

  b. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix D, “Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express”, on page 125 for information about installing and configuring an application server.

3. During installation, you are asked if you want to use /opt as the base directory. If space permits, use /opt as the base installation directory. To accept /opt as the base directory, press Enter.

   Notes:

   a. With the installation of client and server packages, the system prompts you with the query, `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with installation?` These scripts create the IBM Tivoli Directory Server user ID. Type `y` to continue.
   b. If you are installing the server package, you also see the prompt, `Do you want to install these as setuid and/or setgid files?` The programs need to be able to start daemons, run DB2 commands, and create the IBM Tivoli Directory Server DB2 instance user ID and group, so they occasionally need to run as root. Type `y` to continue.
4. When the installation is completed, type `q` to return to the command prompt.
5. If you want to include security functions, install GSKit 7a. See "Installing GSKit".

Installing GSKit

You can install GSKit 7a using either the AdminTool or the command line.

To install GSKit using the **admintool** utility:

1. Log in as **root**.
2. Type the following at a root command prompt: `admintool&`

   The Users window is displayed.
3. Click **Browse** —> **Software**. The Software window is displayed.
4. Click **Edit** —> **Add**. The Set Source Media window is displayed.
5. In the **Path** field, type the full path name to the directory that contains the GSKit installation code. For example, if you are installing from a CD-ROM:

   ```
   /cdrom/cdrom0/gskit
   ```
6. Click **OK**.
7. Select **Certificate and SSL Base Runtime (gsk7bas)**
8. Click **Add**. You are asked if you want to continue the installation.
9. Type `y` and press Enter. After the package is installed, a message is displayed and you are instructed to press Return.
10. Press Enter.
11. When you are finished installing packages, click **File** —> **Exit** to exit the **admintool** utility.

To install GSKit using the command line:

1. Insert the CD.
2. Log in as **root**.
3. At the command prompt, install the required tar file sets with the following command:

   ```
   pkgadd -d /cdrom/cdrom0/gskit
   ```

See Appendix I, "Setting up GSKit to support CMS key databases", on page 139 for more information about setting up GSKit after installation.

Removing GSKit

To remove GSKit, type the following at a command prompt:

```
pkgrm  gsk7bas
```

Chapter 10. Installing IBM Tivoli Directory Server using HP-UX utilities

Attention: If you have a version of IBM Directory Server installed and you want to migrate your data, read and understand the migration process in "Migration from IBM Directory Server Version 4.1 or 5.1 for UNIX installations" on page 42 before installing IBM Tivoli Directory Server 5.2. It is very important that you back up and export previous versions of schema files and the server configuration file before installing IBM Tivoli Directory Server 5.2.

Before installing IBM Tivoli Directory Server

The following sections describe how to set the current configuration parameters and install IBM Tivoli Directory Server. You must have the current kernel configuration parameters set, and Java Runtime Environment 1.4.1 and DB2 Version 7.2 FixPak 5 or later installed before installing IBM Tivoli Directory Server. You can use the **db2_install** command to install the version of DB2 (8.1 FixPak 2) provided. To install HP-UX Runtime Environment for the Java 2 Platform Version 1.4.1, use the instructions provided with the Java package.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information.

Note: Before installing DB2, you must remove any existing versions of DB2 that might have been installed previously. If you try to install DB2 over an existing version of DB2, DB2 does not install correctly. If this occurs you must remove DB2 and then reinstall it.

Setting the current kernel configuration parameters

The following table contains the parameters and values that must be set before installing IBM Tivoli Directory Server.

Table 2. HP-UX operating system kernel configuration parameters

Kernel parameter	Value 256MB+ physical memory
maxuprc	512
maxfiles	256
nproc	1024
nflocks	8192
ninode	2048
nfile	(4 * ninode)
msgseg	32767
msgmnb	65535 (1)
msgmax	65535 (1)
msgtql	1024

© Copyright IBM Corp. 1998, 2003

Table 2. HP-UX operating system kernel configuration parameters (continued)

Kernel parameter	Value 256MB+ physical memory
msgmap	258
msgmni	256
msgssz	16
semmni	512
semmap	514
semmns	1024
semmnu	1020
shmmax	268435456 (2)
shmseg	16
shmmni	300
max_thread_proc (Only if using the Web Administration Tool)	1024
maxusers (Only if using the Web Administration Tool)	256

Note: After you update the max_thread_proc and maxusers parameters, be sure that the nproc parameter is set to 2068 or more, and the nkthread parameter to 3635 or more.

To set a kernel configuration parameter:

1. At a command prompt, type: `sam`

   The System Administration Manager opens.
2. Double-click **Kernel Configuration**.
3. Double-click **Configurable Parameters**.
4. Double-click the parameter you want to edit and type the new value in the **Enter New Formula/Value** field. Click **OK**.
5. Repeat step 4 for each parameter that needs to be set.
6. Click **Actions —> Process New Kernel**.
7. To process the modifications, click **Yes**.
8. Select **Move Kernel Into Place and Shutdown/Reboot Now** and click **OK**.

Installing IBM Tivoli Directory Server

Before installing IBM Tivoli Directory Server, remove any non-IBM versions of LDAP that might have been installed previously. If you try to install IBM Tivoli Directory Server over an existing non-IBM version of LDAP, such as OpenLDAP, IBM Tivoli Directory Server might not install correctly. If this occurs you must remove IBM Tivoli Directory Server and then reinstall it. See "Uninstalling IBM Tivoli Directory Server" on page 100.

Before installing IBM Tivoli Directory Server, be sure that you have the correct kernel configuration parameters set, and Java Runtime Environment 1.4.1 and DB2 Version 7.2 FixPak 5 or later installed.

The instructions in this section assume that you are logged in as **root** and have the IBM Tivoli Directory Server Version 5.2 CD mounted at /SD_CDROM.

To install IBM Tivoli Directory Server:

1. Type `swinstall` at a command prompt.

   Note: **swinstall** does not automatically read the CD. You need to supply the full path to the install image. The path to the client-server package is /SD_CDROM/ldap52_us/hpux11_ibmldap52servers.depot.

   You can install the following packages:

   Server/client
   hpux11_ibmldap52servers.depot

   Client only
   hpux11_ibmldap52clients.depot
2. Select the IBM Tivoli Directory Server 5.2 package you want to install. You can select from the following list:
   - **LDAPServer** to install both the server and client.
   - **LDAPClient** to install the client only.
   - **ids_tools** to install the Web Administration Tool.
3. Click **Actions —> Mark For Install**.
4. Click **Actions —> Install (analysis)**. Analysis is complete when the Status field reads **Ready**.
5. Click **OK**.
6. Click **Yes** to begin installation. Installation is complete when the Status field reads **Done**.
7. Click **File —> Exit**.

Notes:

1. To enable SSL, you must also install GSKit. See "Installing GSKit".
2. If you install the Web Administration Tool, DSML files are also copied to your computer. See Appendix F, "Installing and configuring DSML", on page 131 for information about installing and configuring DSML.
3. If you install the Web Administration Tool, an application server such as the embedded version of WebSphere Application Server - Express is required to run the tool. See Appendix D, "Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express", on page 125 for information about installing and configuring an application server.

Installing GSKit

You can install the GSKit package (gsk7bas.tar.Z) through the command line or through **sam**, a GUI utility for system administration.

To install GSKit:

1. Download or copy the GSKit package to /tmp.
2. Run the following command to change to the /tmp directory:

```
cd /tmp
```

3. Uncompress and untar the package:
```
 zcat gsk7bas.tar.Z | tar -xvf - cd
```
4. Run the following command to install:
```
swinstall  -s /var/spool/pkg/gsk7bas gsk7bas
```

   where
   - **-s** specifies the full_path of the software source.
   - **gsk7bas** contains the Restricted GSKit Base Toolkit install image.

See Appendix I, "Setting up GSKit to support CMS key databases", on page 139 for more information about setting up GSKit after installation.

Setting system variables for HP-UX

Set or verify that the following path has been set in your `.profile`.

```
SHLIB_PATH=/usr/lib
```

For example:

```
export SHLIB_PATH=/usr/lib;$SHLIB_PATH
```

To set the language support environment variables, run the following command:

```
echo 'export NLSPATH=/usr/lib/nls/msg/%L/%N' >>~/.profile
```

Note: Be sure to include the tilde character before `/.profile`.

Removing GSKit

To remove GSKit, run the following command at a command prompt:

```
swremove gsk7bas
```

Chapter 11. Installing on Windows platforms using silent installation

This chapter provides instructions for installing IBM Tivoli Directory Server 5.2 on a Windows computer using silent installation, and for installing and uninstalling GSKit from the command line on Windows.

Silent installation

Silent installation installs IBM Tivoli Directory Server with no user input required during installation.

The following options and conditions apply to silent installation:

- You must have at least 100 MB of memory free before invoking silent installation.
- You do not need to install both the client and the server. You can choose to install the client only.
- Silent installation does not install DB2, GSKit, or the embedded version of WebSphere Application Server - Express.
- Be sure that you have at least 100 MB of free space in the directory specified by the TEMP environment variable.
- If you choose to install the server, you must already have DB2 installed.
- If the client is already installed, you can add the server in a later installation.
- If the server is selected for installation in the options file, the client will automatically be installed if it is not there, regardless of whether it was selected for installation in the options file.
- The Web Administration Tool can be installed whether or not the server or client is installed.
- To edit installation path settings, copy the InstallServer.txt file from the optionsFile directory to a writable location.

To begin installing the IBM Tivoli Directory Server 5.2 using silent installation:

1. If you are installing from the CD, insert the CD in your CD-ROM drive and go to the CD-ROM drive. Otherwise, change to the directory where the downloaded IBM Tivoli Directory Server file was unzipped.
2. At a command prompt, type the following:

   ```
   cd \ismp
   consoleSetup -is:silent -options d:\ismp\optionsFiles\InstallServer.txt
   ```

   where *d*: is the CD-ROM drive or the drive where you unzipped the file.

   Note: If you want to specify an additional log file, type the following:

   ```
   consoleSetup -is:silent -options d:\ismp\optionsFiles\InstallServer.txt
         -log !c:\mydirectory\ldapinst.log @ALL
   ```

   c:\mydirectory\ldapinst.log can be changed to point to where you want to place the log file. The log file will still be created in the target installation directory. The default location is C:\Program Files\IBM\LDAP\ldapinst.log.

© Copyright IBM Corp. 1998, 2003

Note: You must use consoleSetup.exe rather than setup.exe because only consoleSetup.exe returns a return code.

3. IBM Tivoli Directory Server is installed with no further input. If the installation exits for any reason, you can find information about the exit by viewing the return code or checking the *installpath*\ldapinst.log file. (*installpath* is the path where you installed IBM Tivoli Directory Server.)

   Check the return code by checking the value of %ERRORLEVEL% from a .bat file. A return code of 0 indicates that the installation was successful. A non-zero return code indicates that the installation failed. See "Checking the return code" for a list of return codes.

   Installation is complete when control returns to the command line or to the invoking program.

   If installation is unsuccessful, check to be sure that your options file settings and command-line parameters are valid.
4. After installation, restart the system. If you are also installing other products, you can restart at an appropriate time. If the server was installed, you must configure before the server is usable. You can use the **ldapcfg** command line utility to configure silently. See "Using the ldapcfg utility" on page 92 for information.

Verifying the silent installation

To verify that the silent installation was successful, you can check the return code and the log file.

Common reasons for the silent installation failing are:

- A previous or current version of IBM Tivoli Directory Server is already installed.
- The prerequisites are not present. The server requires a valid version of DB2.
- There is not enough disk space to install.
- The options file is incorrect. Be very careful when editing the options file. There cannot be blank lines or control characters in the file. If the installation exits with no log file, this is usually because the options file is invalid (with blank lines, for example), or because the path to the options file was specified incorrectly.

Checking the return code

The %ERRORLEVEL% variable contains the return code. The following return codes can be received:

- `3001 Prerequisites missing`
- `3002 Java exception`
- `3003 No feature selected for silent install`
- `3004 Attemping to install wrong level or existing level. Only current over current allowed`

Other return codes might be returned from the InstallShield program.

Checking the log file

To verify that silent installation was successful using the log file:

1. Check the log file to see if it exists in the target directory. If the log is not there, the installation failed, and you can refer to the log file that was specified on the silent installation command with the **-log** option to see why the installation failed.
2. Check the log file for the string **Exiting LdapExit**.

3. Verify that the installation was completed by checking the Windows registry. The following text should be in the registry, depending on which components were installed:

   In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP\

   ```
   ClientMajorVersion 5.2
   ServerMajorVersion 5.2
   WebadminMajorVersion 5.2
   ```

   In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP\Client\

   ```
   ClientMinorVersion 0.0
   LDAPHome install_location
   ```

   In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP\Webadmin\

   ```
   WebadminMinorVersion 0.0
   LDAPHome install_location
   ```

   In HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP\Server\

   ```
   ServerMinorVersion 0.0
   LDAPHome install_location
   ```

Options file for silent installation

The following text is in the options file provided with IBM Tivoli Directory Server:

```
#Sample response file for the Server/Client package
#(Lines beginning with # are comments)
# Be sure there are no blank lines in this file!
#
# The following 3 lines MUST be present, and NOT modified
-silent
-G createDirectoryResponse="yes"
-G replaceExistingResponse="yesToAll"
#
# install destination - this can be modified to install location
-P product.installLocation="C:\Program Files\IBM\ldap"
#
# Select the features to install. Note: if the server is selected, the
# client will automatically be installed. To deselect a feature, set the
# field to false.
-P ServerFeature.active=true
-P ClientFeature.active=true
-P WebadminFeature.active=true
##############################################################################
#
# Selected Locales
#
# The list of selected locales. This list determines which locale-specific
# components are installed for the product. Legal values are:
#
#    en    - English
#    fr    - French
#    de    - German
#    it    - Italian
#    ja    - Japanese
#    ko    - Korean
#    pt_BR - Portuguese (Brazil)
#    zh    - Simplified Chinese
#    es    - Spanish
#    zh_TW - Traditional Chinese
#
# For example, to select English, use
#
#    -P selectedLocales=en
#
```

```
#
#
-P selectedLocales=en
# This must be last line. Be sure no blank lines or carriage controls follow!
# This must be last line. Be sure no blank lines or carriage controls follow!
```

You can edit the following line to point to the desired target installation directory:

```
-P product.installLocation="C:\Program Files\IBM\ldap"
```

The features lines can be edited to disable a feature from being installed. For example, `-P WebadminFeature.active=true` can be changed to `-P WebadminFeature.active=false` to indicate that you do not want to install the IBM Tivoli Directory Server Web Administration Tool.

You can specify the correct locale by editing the following line:

```
-P selectedLocales=en
```

Change `en` to the language you want to install.

Installing GSKit on Windows operating systems

If you install IBM Tivoli Directory Server using silent installation, GSKit is not installed. You can use the following procedure to install it.

To install GSKit 7a:

1. Extract the files from the self-extracting GSKit file by typing the following at a command prompt in the directory where the gsk7bas.exe file is located:

   ```
   gsk7bas.exe path /D
   ```

   where
   - *path* is the directory where you want to extract the files
   - /D specifies that you want to create directories
2. In the directory where you extracted the files, run the following command:

   ```
   setup LDAP path -s -f1"extracted file location\setup.iss"
   ```

   where
   - LDAP is the name of your application and will be registered as a registered user of GSK in the Windows Registry (under the key SOFTWARE\\IBM\\GSK\\REGAPPS).
   - *path* is the path where you want to install GSKit. Note that the installation program appends \ibm\gsk7 to any path you enter.

     Note: Do not start setup.exe by clicking on the icon.

   The following options can be used:
   - **-s** to run the setup in the silent mode.
   - **-f1***extracted file location*\setup.iss specifies the response file needed to run the setup in the silent mode. Note that there is no space between **-f1** and the beginning of the extracted file location.

For example:

```
setup LDAP gskit -s -f1"d:\temp\setup.iss"
```

See Appendix I, “Setting up GSKit to support CMS key databases”, on page 139 for more information about setting up GSKit after installation.

Removing GSKit

To remove GSKit, run the following command:

```
gsk7BUI LDAP
```

Chapter 12. Configuration

You can use either the Configuration Tool (**ldapxcfg**) or the **ldapcfg** command-line utility to configure the server. **ldapucfg** is used to unconfigure the server through the command line.

You must have at least 80 MB of hard disk space available to configure the database.

If you used the InstallShield GUI to install, the Configuration Tool is started after installation (and after system restart on a Windows system).

After installation, if configuration does not start automatically, you must use the Configuration Tool or the command line configuration program to do the following tasks:

- Define the IBM Tivoli Directory Server administrator distinguished name (DN) and password. This operation can be compared to defining the root user ID and password on a UNIX system.
- Configure the database.

Note: After you configure, see Chapter 13, "After you install and configure", on page 97 for information about:

  - Starting the server
  - Starting the embedded version of WebSphere Application Server - Express service if you want to use the Web Administration Tool

  You can find more information in the *IBM Tivoli Directory Server Version 5.2 Administration Guide*.

In addition, you can use the Configuration Tool for the following tasks:

- Configuring (or reconfiguring) and unconfiguring the database
- Enabling and disabling the change log
- Adding and removing suffixes
- Adding and removing schema files
- Importing and exporting LDIF data
- Backing up, restoring, and optimizing the database

Note: If you are configuring a UNIX-based system, you must run the configuration utilities (**ldapcfg** and **ldapxcfg**) from a directory that has execute permission for **other**. That is, the directory must have at least the **--------x** permission set. If this permission is not set, you might see an error message and experience a subsequent failure during the database creation step. To set this permission for your current directory, you can enter the command:

```
chmod o+x .
```

The period (.) in the command is required to indicate the current directory.

Using the IBM Tivoli Directory Server Configuration Tool (ldapxcfg)

To configure IBM Tivoli Directory Server using the Configuration Tool:

1. On a UNIX system, log in as **root**. On a Windows system, log on as any user in the Administrators group.
2. Type `ldapxcfg` at a command prompt. Alternatively, on a Windows system, you can click **Start —> Programs —> IBM Tivoli Directory Server 5.2 —> Directory Configuration**.
3. The Configuration Tool window is displayed.

   Note: If you are using a Windows platform, do not minimize the Configuration Tool window or the command prompt window that is displayed during initial configuration, or unpredictable results might occur.

   In the task list on the left, click the task you want to perform. For information about performing a task, see the section shown in the following list:

   Set or change the Administrator DN and password
   See "Setting the Administrator DN and password".

   Configure the database
   See "Configuring the database" on page 86.

   Unconfigure the database
   See "Unconfiguring the database" on page 87.

   Configure or unconfigure the change log
   See "Enabling or disabling the change log" on page 87.

   Manage suffixes
   See "Managing suffixes" on page 88.

   Manage schema files
   See "Managing schema files" on page 89.

   Import LDIF data
   See "Importing LDIF data" on page 90.

   Export LDIF data
   See "Exporting LDIF data" on page 91.

   Back up database
   See "Backing up the database" on page 92.

   Restore database
   See "Restoring the database" on page 92.

   Optimize database
   See "Optimizing the database" on page 92.
4. Close the Configuration Tool when you have completed all configuration tasks.

Setting the Administrator DN and password

To set the administrator DN and password:

1. In the IBM Tivoli Directory Server Configuration Tool window, click **Administrator DN/password** in the task list on the left.
2. In the Administrator DN/password window on the right, type a valid DN (or accept the default DN, **cn=root**) in the **Administrator DN** field.

   The IBM Directory Server administrator DN is the DN used by the administrator of the directory. This administrator is the one user who has full access to all data in the directory.

The default DN is **cn=root**. DNs are not case sensitive. If you are unfamiliar with X.500 format, or if for any other reason you do not want to define a new DN, accept the default DN.

3. Type the password for the Administrator DN in the **Administrator Password** field. You must define a password. Passwords are case-sensitive.

   Record the password for future reference.
4. Retype the password in the **Confirm password** field.
5. Click **OK**.

   Note: Double byte character set (DBCS) characters in the password are not supported.

Configuring or unconfiguring the database

When you configure the database, the Configuration Tool adds information about the database that will be used to store directory data to the configuration file (ibmslapd.conf). In addition, if the database does not already exist, the Configuration Tool creates the database.

Notes:

1. Before configuring the database, be sure that the environment variable DB2COMM is **not** set.
2. The server must be stopped before you configure or unconfigure the database.

When you unconfigure the database, the Configuration Tool removes the database information from the configuration file. Based on your selections, it might also delete the database (and all data in it) and remove the instance that contains the database.

Before you configure: creating the DB2 database owner and database instance owner

Before you configure the database, you must create a user ID for the user who will own the DB2 database. The user ID you specify will own the database instance where the DB2 database will exist, and the DB2 instance will be in the user's home directory.

Note: If you want a different database instance name, you must use the **ldapcfg** command with the **-t** option to configure the database. See "Configuring the database" on page 93 for information.

The user ID can be no longer than 8 characters. In addition:

- On Windows platforms, the user must be a member of the Administrators group.
- On UNIX platforms:
  - The user must have a home directory and must be the owner of the home directory.
  - The group ownership of the user's home directory should be the DB2 group created when DB2 was installed. On AIX and Solaris, this group is usually named **dbsysadm**. On zSeries Linux, this group is usually named **db2iadm**. For example, in the case of a user named **ldapdb2**, the user ID home directory should be owned by ldapdb2:dbsysadm on AIX and Solaris or by ldapdb2:db2iadm on zSeries Linux.

    There might be some groups that do not work correctly as the user's primary group when configuring the database. For example, if the user's primary group on Linux is **users**, problems might occur. Use **other** on Linux if you want to be sure that the primary group will work.

The user **root** must be a member of the user's primary group. If **root** is not a member of this group, add **root** as a member of the group.

- For best results, the user's login shell should be the Korn shell script (/usr/bin/ksh).
- The user's password must be set correctly and ready to use. For example, the password cannot be expired or waiting for a first-time validation of any kind. (The best way to verify that the password is correctly set is to telnet to the same computer and successfully log in with that user ID and password.)
- When configuring the database, it is not necessary, but customary, to specify the home directory of the user ID as the database location. However, if you specify some other location, the user's home directory still must have 3 to 4 MB of space available. This is because DB2 creates links and adds files into the home directory of the instance owner (that is, the User) even though the database itself is elsewhere. If you do not have enough space in the home directory, you can either create enough space or specify another directory as the home directory.

Configuring the database

To configure the directory database:

1. In the Configuration Tool, click **Configure database** in the task list on the left.
2. The Configuration Tool attempts to determine whether you already have a database. If you have a database already configured (that is, the information for the database is in the configuration file), the Configuration Tool prompts you for information about what you want to do. For example, if the database is configured but cannot be found on the system, you might choose to create a database using the name specified in the configuration file. Use the information shown in the windows that are displayed to configure the database.

Depending on whether or not you already have a database, some or all of the following windows are displayed.

3. If a user ID and password are requested:
   a. Type a user ID in the **User ID** field. This user ID must already exist before you can configure the database. This is the user ID you created in "Before you configure: creating the DB2 database owner and database instance owner" on page 85. (In previous releases, the user ID was created if it did not exist, but this is no longer true.)
   b. Type a password for the user in the **Password** field. Passwords are case-sensitive.
   c. Click **Next**.
4. If the database name is requested:
   a. Type the name you want to give the DB2 database. The name can be from 1 to 8 characters long. The database will be created in an instance with the same name as the user ID.

      Note: If you want a different database instance name, you must use the **ldapcfg** command with the **-t** option to configure the database. See "Configuring the database" on page 93 for information.
   b. Click **Next**.
5. If the database location is requested:

   a. Type the location for the database in the **Database location** field. For Windows platforms, this must be a drive letter. For non-Windows platforms, the location must be a directory name, such as /home/ldapdb2.

      Be sure that you have at least 80 MB of free hard disk space in the location you specify and that additional disk space is available to accommodate growth as new entries are added to the directory.
   b. Click **Next**.
6. If a character set selection is requested:
   a. Click the type of database you want to create. You can create a UCS Transformation Format (UTF-8) database, in which LDAP clients can store UTF-8 character data, or a local code page database, which is a database in the local code page.

      If you want to use language tags, the database must be a UTF-8 database. For more information about UTF-8, see Appendix H, "UTF-8 support", on page 135
   b. Click **Next**.
7. In the verification window, information is displayed about the configuration options you specified. To return to an earlier window and change information, click **Back**. To begin configuration, click **Finish**.
8. The completion window is displayed. Click **Close**.

Unconfiguring the database

To unconfigure the database:

1. In the Configuration Tool, click **Unconfigure database** in the task list on the left.
2. In the Unconfigure database window, click one of the following:

   Unconfigure only
   Does not destroy any existing LDAP DB2 data. However, the configuration information for the database will be removed from the configuration file (ibmslapd.conf), and the database will be inaccessible to the directory server.

   Unconfigure and destroy database
   Removes the existing database and its contents, and removes the configuration information for the database from the configuration file.

   Unconfigure and destroy database and delete instance
   Removes the existing database and its contents, removes the configuration information for the database from the configuration file, and deletes the instance in which the database is located.

   Attention: Before destroying an instance, be sure that there are no databases in the instance that must be kept.
3. Click **Unconfigure**.

Enabling or disabling the change log

The change log database is used to record changes to the schema or directory entries in the typical LDAP entry structure that can be retrieved through the LDAP API. The change log records all update operations: add, delete, modify, and modrdn. The change log enables an IBM Tivoli Directory Server client application to retrieve a set of changes that have been made to an IBM Tivoli Directory Server database. The client might then update its own replicated or cached copy of the data.

You can use the Configuration Tool to enable or disable the change log.

Note: The server must be stopped before you enable or disable the change log.

Enabling the change log

To enable the change log:

1. In the Configuration Tool, click **Configure/unconfigure changelog** in the task list on the left.
2. In the Configure/unconfigure changelog window, select the **Enable change log database** check box.
3. In the **Maximum number of log entries** box, click **Unlimited** if you want an unlimited number of entries in the change log. If you want to limit the number of entries, click **Entries** and type the maximum number of entries you want recorded. The default is 1,000,000 entries.
4. In the **Maximum age** box, accept the default of **Unlimited** if you want entries to remain in the change log indefinitely, or click **Age** and type the number of days and hours for which you want each entry to be kept.
5. Click **Update**.

Disabling the change log

To disable the change log:

1. In the Configuration Tool, click **Configure/unconfigure changelog** in the task list on the left.
2. In the Configure/unconfigure changelog window, clear the **Enable change log database** check box.
3. Click **Update**.

Managing suffixes

A suffix (also known as a naming context) is a distinguished name (DN) that identifies the top entry in a locally held directory hierarchy. Because of the relative naming scheme used in LDAP, this DN is also the suffix of every other entry within that directory hierarchy. A directory server can have multiple suffixes, each identifying a locally held directory hierarchy; for example, o=ibm,c=us.

Note: The specific entry that matches the suffix must be added to the directory.

Entries to be added to the directory must have a suffix that matches the DN value, such as ou=Marketing,o=ibm,c=us. If a query contains a suffix that does not match any suffix configured for the local database, the query is referred to the LDAP server that is identified by the default referral. If no LDAP default referral is specified, an **Object does not exist** result is returned.

Note: The server must be stopped before you add or remove suffixes.

Adding a suffix

To add a suffix:

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left.
2. In the Manage suffixes window, type the suffix you want to add in the **SuffixDN** field, and click **Add**.
3. When you have added all the suffixes you want, click **OK**.

Note: When you click **Add**, the suffix is added to the list in the **Current suffix DNs** box; however, the suffix is not actually added to the directory until you click **OK**.

Removing a suffix

To remove a suffix:

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left.
2. In the Manage suffixes window, click the suffix you want to remove in the **Current suffix DNs** box, and click **Remove**.
3. When you have selected all the suffixes you want to remove, click **OK**.

   Note: When you click **Remove**, the suffix is removed from the list in the **Current suffix DNs** box; however, the suffix is not actually removed until you click **OK**.

Managing schema files

You can use the Configuration Tool for the following schema file tasks:

- Adding a schema file to the list of schema files that will be loaded at startup
- Removing a schema file from the list of schema files that will be loaded at startup
- Changing the type of validation checking that is done for schema files

Note: The server must be stopped before you add or remove schema files.

Adding a schema file

To add a schema file to the list of schema files that will be loaded at startup:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, type the path and file name of the schema file you want to load at startup. (Alternatively, click **Browse** to search for the file.)
3. Click **Add**.

   Note: When you click **Add**, the schema file is added to the list in the **Current schema files** box; however, the schema file is not actually added until you click **OK**.
4. When you have added all the schema files you want, click **OK**.

Removing a schema file

To remove a schema file from the list of schema files that will be loaded at startup:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, click the schema file you want to remove in the **Current schema files** box.
3. Click **Remove**.

   Notes:

   a. A schema file that contains the string `system` is a system file and cannot be deleted.

   b. When you click **Remove**, the schema file is removed from the list in the **Current schema files** box; however, the schema file is not actually removed until you click **OK**.
4. When you have selected all the schema files you want to remove, click **OK** to process the files.

Changing the type of validation checking that is done

To change the type of validation checking that is done on schema files:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, accept the default schema validation rule in the **Schema validation rules** box, or click the rule you want. You can select one of the following rules:
   - Version 3 (Strict)

     LDAP version 3 strict validation checking is done. With this type of validation checking, all parent object classes must be present when adding entries.
   - Version 3 (Lenient)

     LDAP version 3 lenient validation checking is done. With this type of validation checking, all parent object classes do not need to be present when adding entries.

     This is the default.
   - Version 2

     LDAP version 2 checking is done.
   - None

     No validation checking is done.
3. Click **OK**.

Importing and exporting LDIF data

You can use the Configuration Tool to import data from an LDAP Data Interchange Format (LDIF) file or to export data from the database to an LDIF file. LDIF is used to represent LDAP entries in text form. When importing, you can add entries to an empty directory database or to a database that already contains entries. You can also use the Configuration Tool to validate the data in the LDIF file without adding the data to the directory.

Importing LDIF data

Notes:

1. Before you import the data from an LDIF file, be sure to add any necessary suffixes. See "Adding a suffix" on page 88 for information about adding a suffix.
2. The server must be stopped before you import LDIF data.

To import data from an LDIF file:

1. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
2. In the Import LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. Click **Standard import** if you want to import the data using the **ldif2db** utility, or click **Bulkload** if you want to import the data using the **bulkload** utility.

   Note: For large LDIF files, the **bulkload** utility is a faster alternative to **ldif2db** if you are importing a large number of entries.
4. If you want trailing spaces removed from the data, select the **Remove trailing spaces in Standard import or Bulkload** check box.

5. If you clicked **Bulkload**, click the type or types of checking you want to perform on the LDIF data in the **Bulkload options** box. You can select one or more of the following:
   - Enable schema checking
   - Enable ACL checking
   - Enable password policy

   Click **Import**.

Note: After loading large amounts of data, especially after populating the database using **bulkload**, be sure to optimize the database. This can make a significant improvement to the performance of the database

Validating LDIF data without adding it to the database

To validate the data in the LDIF file without adding it to the database:

1. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
2. In the Import LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. Click **Data validation only**.
4. Click **Import**.

Exporting LDIF data

Before you export LDIF data, be sure that you have enough space to export all the data.

To export data from the database to an LDIF file:

1. In the Configuration Tool, click **Export LDIF data** in the task list on the left.
2. In the Export LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. If you want to overwrite the data in an existing file, select the **Overwrite if file exists** check box.
4. If you want to export the creatorsName, createTimestamp, modifiersName, and modifyTimestamp operational attributes, select the **Export operational attributes** check box.

   These operational attributes are created and modified by the server when a directory entry is created or modified; they are also modified any time the entry is modified. They contain information about the user who created or modified the entry and the time the entry was created or modified.
5. If you want to export only some of the data in the directory, complete the **Subtree DN** field. The subtree DN identifies the top entry of the subtree that is to be written to the LDIF output file. This entry, plus all entries below it in the directory hierarchy, are written to the file. If you do not specify this option, all directory entries stored in the database are written to the output file based on the suffixes specified in the IBM Directory Server configuration file.
6. Click **Export**.

Backing up, restoring, and optimizing the database

You can use the Configuration Tool for the following database tasks:

- Backing up the data in the database

- Restoring data and, optionally, configuration settings that were previously backed up
- Updating statistics related to the data tables for the purpose of improving performance and query speed

Backing up the database

The server must be stopped before you can back up the database.

To back up the database:

1. In the Configuration Tool, click **Backup database** in the task list on the left.
2. In the Backup database window on the right, in the **Backup directory** field, type the directory path in which to back up all directory data and configuration settings. Alternatively, click **Browse** to locate the directory path.
3. Click one of the following:
   - **Create backup directory as needed** if you want the directory to be created if it does not exist.
   - **Abort if backup directory is not found** if you do not want the directory you specified to be created. If this directory does not exist and you select this option, the database will not be backed up.
4. Click **Backup**.

Restoring the database

The server must be stopped before you can restore the database.

To restore the database:

1. In the Configuration Tool, click **Restore database** in the task list on the left.
2. In the Restore database window on the right, in the **Backup directory** field, type the path in which the directory was previously backed up. Alternatively, click **Browse** to locate the path.
3. If you want to restore only the directory data, but not the configuration settings, select the **Restore data only (not configuration settings)** check box. If you want to restore both data and configuration settings, be sure the check box is cleared.
4. Click **Restore**.

Optimizing the database

The server must be stopped before you can optimize the database.

Optimize the database to update statistics related to the data tables; this can improve performance and query speed. Perform this action periodically or after heavy database updates; for example, after importing database entries.

1. In the Configuration Tool, click **Optimize database** in the task list on the left.
2. In the Optimize database window on the right, click **Optimize**.

Using the ldapcfg utility

The **ldapcfg** utility is a command-line tool that you can use to configure IBM Tivoli Directory Server. You can use **ldapcfg** instead of the Configuration Tool for the following tasks:

- Setting the administrator DN and password. See "Setting the administrator DN and password" on page 93 for instructions.
- Configuring a database. See "Configuring the database" on page 93 for instructions.

- Changing the password of the DB2 administrator in the server configuration file. See "Changing the DB2 administrator password" on page 95 for instructions.
- Enabling the change log. See "Enabling the change log" on page 95 for instructions.
- Adding a suffix. See "Adding a suffix" on page 95 for instructions.

Setting the administrator DN and password

To define the administrator DN and password, type the following at a command prompt:

```
ldapcfg -u "adminDN" -p password
```

where

- *adminDN* is the administrator DN you want.
- *password* is the password for the administrator DN.

Note: Double byte character set (DBCS) characters in the password are not supported.

For example:

```
ldapcfg -u "cn=root" -p secret
```

Note: Do not use single quotation marks (') to define DNs with spaces in them. They are not interpreted correctly.

To accept the default administrator DN of cn=root and define a password, type the following command at a command prompt:

```
ldapcfg -p password
```

where *password* is the password for the administrator DN.

For example:

```
ldapcfg -p secret
```

Configuring the database

When you configure the database, you must always specify a user ID and password on the command line. The instance name is, by default, the same as the user ID. The user ID must already exist and must meet certain requirements. If you want a different instance name you can specify it using the **-t** option. This name must also be an existing user ID that meets certain requirements. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for information about these requirements on both Windows and UNIX platforms.

Attention:

1. Before configuring the database, be sure that the environment variable DB2COMM is **not** set.
2. Be sure to read this section before you use the **ldapcfg** command. Some options (such as **-f** and **-s**) have changed. Unpredictable results will occur if you use them incorrectly or as they were used in previous releases.
3. The server must be stopped before you configure the database.

To configure a database, the following options are available:

-l *location*
Specifies the location of the DB2 database. For UNIX systems, this is a directory name such as /home/ldapdb. For Windows systems, this is a drive letter such as C:

-a *id* Specifies the DB2 administrator ID.

-c Creates a database in UTF-8 format. (The default, if you do not specify this option, is to create a database that is in the local code page.)

-i Destroys any instance currently configured with IBM Tivoli Directory Server. All databases associated with the instance are also destroyed.

-w *password*
Specifies the DB2 administrator password.

Note: The **ldapcfg -w** *password* command no longer changes the system password of the database owner. It only updates the ibmslapd.conf file. See "Changing the DB2 administrator password" on page 95 for information about using the **-w** option alone.

-d *database*
Specifies the DB2 database name.

-t *dbinstance*
Specifies the database instance. If you do not specify an instance, the instance name is the same as the DB2 administrator ID.

-o Overwrites the database if one already exists. By default, the database being overwritten is not deleted.

-r Destroys any database currently configured with IBM Tivoli Directory Server.

-f Specifies the full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors will be sent to the file.

-q Runs in quiet mode. All output is suppressed except for errors.

-n Runs in no prompt mode. All output is generated except for messages requiring user interaction.

To configure a database on /home/ldapdb2 with a DB2 administrator name of **db2admin**, a password of **mypassword**, and a database name of **dbName** when there is not an existing database configured (that is, the first time), the command is:

```
ldapcfg -l /home/ldapdb2 -a db2admin -w mypassword -d dbName
```

To configure a database on /home/ldapdb2 with a DB2 administrator name of **db2admin**, a password of **mypassword**, a database name of **dbName**, and an instance name of **dbInstance** when there is not an existing database configured (that is, the first time), the command is:

```
ldapcfg -l /home/ldapdb2 -a db2admin -w mypassword -d dbName -t dbInstance
```

To configure a database on /home/ldapdb2 when a database is already configured and you want to overwrite it, the command is:

```
ldapcfg -l /home/ldapdb2 -a db2admin -w mypassword -d dbName -o
```

For information about unconfiguring a database using the **ldapucfg** command-line utility, see "Unconfiguring the database" on page 99.

Changing the DB2 administrator password

If you change the password for the DB2 administrator through the operating system, you must also change it using **ldapcfg** with the **-w** option. This changes the password in the server configuration file. Similarly, if you change the password for the DB2 administrator with the **ldapcfg** command, you must also change it through the operating system.

To change the DB2 administrator password to **newpassword**, type the following command:

```
ldapcfg -w newpassword
```

Note: Double byte character set (DBCS) characters in the password are not supported.

Enabling the change log

To enable the change log use the **-g** option. The change log is a separate database that records changes to the main directory. You need an additional 30 MB to create it.

Note: The server must be stopped before you enable the change log.

To set the maximum number of entries that will be logged in the change log, use the **-m** *maxentries* option. If you do not specify a maximum number, the default of 0 means there is no limit to the number of entries.

To set the time for which entries will be kept in the change log, use the **-y** *maxdays* **and -h** *maxhours* options. For example, to set the age limit to 30 days and 12 hours, type `ldapcfg -y 30 -h 12`.

For information about disabling the change log using the **ldapucfg** command-line utility, see "Unconfiguring the database" on page 99.

Adding a suffix

To add suffixes to the ibmslapd.conf file using the **ldapcfg** utility, the command is:

```
ldapcfg -s "suffix"
```

where *suffix* is the suffix you want to add.

Note: The server must be stopped before you add suffixes.

Importing or exporting data

To import data from an LDIF file, you can use either the **ldif2db** or the **bulkload** utility.

To export data to an LDIF file, you can use the **db2ldif** utility.

See the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for instructions.

Backing up, restoring, and optimizing the database

The following sections describe how to back up, restore, and optimize the database using command line utilities.

Backing up the database using the dbback command

To back up the directory database using the command line, use the **dbback** utility.

Notes:

1. The server must be stopped before you back up the database.
2. This utility uses the ibmslapd.conf configuration file.

The following options are available:

-d *directory*
: Specifies the directory in which you want to back up the database. The user ID that owns the configured directory database must have write access to this directory.

-w *filename*
: Specifies the full path and file name of a file into which you want to redirect output.

Restoring the database using the dbrestore command

To restore the directory database using the command line, use the **dbrestore** utility.

Note: The server must be stopped before you restore the database.

The following options are available:

-d *directory*
: Specifies the directory from which to restore the database.

-n
: Specifies not to restore the ibmslapd.conf file.

-w *filename*
: Specifies the full path and file name of a file into which you want to redirect output.

Optimizing the database using the runstats command

To optimize the directory database using the command line, use the **runstats** command. This command updates statistics related to the data tables.

Note: The server must be stopped before you optimize the database.

The following option is available:

-f *config_file_name*
: Specifies the name of the configuration file. If not specified, ibmslapd.conf is used.

Chapter 13. After you install and configure

After you install the server, set the administrator DN and password, and configure the database, you can start the directory server. If you installed the Web Administration Tool and the embedded version of WebSphere Application Server - Express, you can start the application server.

Starting the directory server

To start the directory server, type `ibmslapd` at a command prompt.

On Windows systems, you can also start and stop the server through the **Services** folder.

- To start the server, click **IBM Tivoli Directory Server V5.2**. Then click **Actions —> Start**.
- To stop the server, click **IBM Tivoli Directory Server V5.2**. Then click **Actions —> Stop**.

For information about starting and stopping the server and performing other administrative tasks using the Web Administration Tool and the command line, see the *IBM Tivoli Directory Server Version 5.2 Administration Guide*.

Starting the application server to use the Web Administration Tool

To start the application server if you are using the embedded version of WebSphere Application Server - Express as your application server:

1. Go to the bin subdirectory of the directory where you installed the embedded version of WebSphere Application Server - Express. If you used the InstallShield GUI to install, this is the appsrv/bin subdirectory of the directory where you installed IBM Tivoli Directory Server.
2. Type one of the following at a command prompt.
   - `startServer server1.bat` for Windows systems
   - `startServer.sh server1` for UNIX systems

Stopping the application server

Use one of the following commands to stop the application server:

- On Windows systems:
  ```
  WASPath\bin\stopServer.bat server1
  ```
- On UNIX systems:
  ```
  WASPath/bin/stopServer.sh server1
  ```

where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express.

Starting the Web Administration Tool

To start the Web Administration Tool:

1. After you have started the application server, from a Web browser, type the following address: http://localhost:9080/IDSWebApp/IDSjsp/Login.jsp

© Copyright IBM Corp. 1998, 2003

The IBM Tivoli Directory Server Web Administration login page window is displayed.

Note: This address works only if you are running the browser on the computer on which the Web Administration Tool is installed. If the Web Administration Tool is installed on a different computer, replace **localhost** with the hostname or IP address of the computer where the Web Administration Tool is installed.

For information about using the Web Administration Tool, see the *IBM Tivoli Directory Server Version 5.2 Administration Guide*.

Chapter 14. Unconfiguring the database and uninstalling IBM Tivoli Directory Server

To remove IBM Tivoli Directory Server from your computer, you must first unconfigure the database, and then uninstall the server. Use the sections in this chapter to unconfigure and remove the server.

Unconfiguring the database

You can use the Configuration Tool (**ldapxcfg**) to unconfigure the database. See "Unconfiguring the database" on page 87 for information.

The options for the **ldapucfg** utility are similar to those for the **ldapcfg** utility. (See "Using the ldapcfg utility" on page 92 for information about **ldapcfg**.) However, in the **ldapucfg** utility:

- The **-d** option removes the currently configured DB2 database. It also removes the change log if enabled.
  - The **-r** option, used with **-d**, destroys any database currently configured with IBM Tivoli Directory Server without prompting for information.
  - The **-i** option, used with **-d**, destroys any instance currently configured with IBM Tivoli Directory Server without prompting for information. All databases associated with the instance are destroyed also.
- The **-g** option disables the change log. Disabling the change log removes the change log database and any data (change records) that are in it. The **-g** option does not affect the main directory database.

Note: If you are unconfiguring a UNIX-based system, you must run **ldapucfg** from a directory that has execute permission for **other**. That is, the directory must have at least the **--------x** permission set. If this permission is not set, you might see an error message and experience a subsequent failure. To set this permission for your current directory, you can enter the command:

```
chmod o+x .
```

The period (.) in the command is required to indicate the current directory.

Attention: Back up any existing schema files and your directory before performing the following steps.

To remove the DB2 configuration information:

1. On UNIX platforms, log in as **root**. On Windows systems, log on as an administrator.
2. Stop all clients that are connected to the IBM Tivoli Directory Server server.
3. Use the **ldapucfg** utility to remove the DB2 configuration information from the server. At the command prompt, enter:

   ```
   ldapucfg -d
   ```

   You might be prompted for more information about removing the database and the DB2 instance.

© Copyright IBM Corp. 1998, 2003

Uninstalling IBM Tivoli Directory Server

After you unconfigure, use the following sections to uninstall IBM Tivoli Directory Server.

Uninstalling using the InstallShield GUI

The following sections describe how to uninstall the IBM Tivoli Directory Server using the InstallShield GUI.

Notes:

1. If you installed IBM Tivoli Directory Server using the InstallShield GUI, use the InstallShield GUI to uninstall.
2. Before you uninstall the embedded version of WebSphere Application Server - Express, you must stop the application server. (See "Stopping the application server" on page 97 for information.) Before you start to uninstall, close all windows to make sure that the *installpath*/appsrv directory is not in use.

   After uninstalling embedded version of WebSphere Application Server - Express, verify that the *installpath*/appsrv directory is removed. If it is not, you must remove it before you attempt to install again.

Windows platforms

To remove IBM Tivoli Directory Server on a Windows platform using the InstallShield GUI:

1. Click **Start —> Settings —> Control Panel —> Add/Remove Programs**.
2. Select **IBM Tivoli Directory Server 5.2**. Click **Change/Remove**.
3. Select the language you want to use during the uninstallation procedure. Click **OK**.
4. On the Welcome window, click **Next**.
5. Select the features you want to uninstall. Click **Next**.

   Note: If you migrated from an IBM Directory Server 4.1 installation in which the DMT and Java feature was installed, **DMT and Java** is in the list of features to be uninstalled. Select this feature to be removed. Until you remove this feature with the InstallShield GUI, it will continue to display in the list of features to uninstall.
6. On the confirmation window, to uninstall the selected features, click **Next**.

UNIX platforms

Note: The InstallShield GUI is not available on iSeries Linux, pSeries Linux, zSeries Linux, and HP-UX.

To remove IBM Tivoli Directory Server on a UNIX platform using the InstallShield GUI:

1. At a command prompt, go to the IBM Tivoli Directory Server `_uninst` directory.
   - On AIX and Linux operating systems, this directory is/usr/ldap/_uninst.
   - On the Solaris operating system, this directory is /opt/IBMldapc/_uninst.
2. Run the uninstall command:

   ```
   ./uninstall
   ```
3. Select the language you want to use during the uninstallation. Click **OK**.
4. On the Welcome window, click **Next**.
5. Select the features you want to uninstall. Click **Next**.

6. On the confirmation window, to uninstall the selected features, click **Next**.

Uninstalling using operating system utilities

After you remove the configuration information, you can uninstall IBM Tivoli Directory Server.

Notes:

1. If you installed IBM Tivoli Directory Server using the InstallShield GUI, uninstall using the process in "Uninstalling using the InstallShield GUI" on page 100.
2. Removing IBM Tivoli Directory Server does not remove any databases you created using IBM Tivoli Directory Server.

AIX operating system

To uninstall the IBM Tivoli Directory Server server or client, type the following:

```
installp -u ldap
```

This removes only IBM Tivoli Directory Server filesets. It does not remove other components such as DB2.

Linux operating system

Before removing IBM Tivoli Directory Server, ensure that the server is stopped and then issue the following commands.

Note: If the IBM Tivoli Directory Server server is installed, you must remove the server before you remove the client (the reverse order of the installation).

```
rpm -ev ldap-server-5.2-1
rpm -ev ldap-webadmin-5.2-1
rpm -ev ldap-client-5.2-1
rpm -ev ldap-msg-xxx-5.2-1.i386.rpm (Where xxx is
language dependent.)
rpm -ev ldap-html-xxx-5.2-1.i386.rpm (Where xxx is
language dependent.)
```

Solaris operating system

You can uninstall IBM Tivoli Directory Server using the **admintool** utility or from a command line using **pkgrm**.

AdminTool removal: To remove IBM Tivoli Directory Server using the admintool utility:

1. Log in as **root**.
2. Type the following at a command prompt:
   ```
   admintool&
   ```
   The **Users** window is displayed.
3. Click **Browse —> Software**. The Software window is displayed.
4. Select the packages to delete from the displayed list.
   ```
   IBM Tivoli Directory Client
   IBM Tivoli Directory Documentation
   IBM Tivoli Directory Messages
   IBM Tivoli Directory Server
   IBM Tivoli Directory Webadmin
   ```
5. Click **Edit —> Delete**. The AdminTool: Warning window is displayed.
6. Click **Delete**.

Note: With the removal of client and server packages, the system prompts you with the query, `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with the removal of this package?` Type `y` to continue. If you are removing the Server package, you also see the prompt, `Do you want to remove these as setuid and/or setgid files?` Type `y` to continue.

7. After the package is removed, the Software window is displayed. When the removal is complete, type `q` to return to the command prompt.

Installing IBM Tivoli Directory Server using the default settings creates the opt/IBMldaps and opt/IBMldapc directories. If you uninstall IBM Tivoli Directory Server, the removal procedure might not remove these directories. If one or both of these directories exist, they create a problem if you later reinstall IBM Tivoli Directory Server in non-default directories.

To ensure that the directories are completely removed issue this command at a command line:

```
rm -fr /opt/IBMldaps /opt/IBMldapc
```

You can now reinstall IBM Tivoli Directory Server to a non-default directory.

Note: This problem does not occur if you reinstall to the default directories.

Command line removal: To see what IBM Tivoli Directory Server components are installed, type:

```
pkginfo | grep -i ibml
```

The output displayed is similar to the following:

```
IBMldapc    IBM Tivoli Directory Client
(sparc) 5.2.0.0
IBMldaps     IBM Tivoli Directory Server
      (sparc) 5.2.0.0
IBMldixxx    IBM Tivoli Directory documentation
 (sparc) 5.2.0.0
IBMldmxxx    IBM Tivoli Directory messages
(sparc) 5.2.0.0
IBMldapw                        IBM Tivoli Directory Webadmin
(sparc) 5.2.0.0
```

Use **pkgrm** to remove the desired packages. For example:

```
pkgrm IBMldaps IBMldapc IBMldapw
```

You can specify either the package name or its listing number. Remove the packages in the reverse order of the installation sequence. (The order in which you remove the Web Administration Tool is not important.)

HP-UX

To remove IBM Tivoli Directory Server, complete the following steps:

1. At a command prompt, type `swremove`
2. Select the installed IBM Tivoli Directory Server.
3. Click **Actions —> Mark For Remove**.
4. Click **Actions —> Remove/Uninstall**.
5. Click **OK**.
6. When removal is complete, click **Done**.

7. Click **File —> Exit**.

Chapter 15. Troubleshooting

If you are having problems installing or configuring IBM Tivoli Directory Server 5.2, refer to this section for possible fixes.

InstallShield GUI installation

If installation does not complete, the first place you can look for information is the ldapinst.log file. If the installation destination directory (*install_directory*) was created, this log is in the *install_directory* root directory. For example, on a Windows system, the ldapinst.log file is, by default, in c:\Program Files\IBM\LDAP\. If *install_directory* was not created before the installation failed, the log might be in a temporary directory. To find it, search for "ldapinst.log". Review this log for any messages about why the installation failed.

Because some of the LDAP features require corequisite products, it is possible that a failure in a corequisite installation caused the IBM Tivoli Directory Server installation to fail. For example, if the server feature is being installed, but the DB2 installation fails, the server feature cannot be installed.

Logs used by the InstallShield GUI when installing embedded version of WebSphere Application Server - Express are:

On Windows platforms

- Documents and Settings*userid*\Local Settings\Temp\installApp.log
- Documents and Settings*userid*\Local Settings\Temp\installAppErr.log
- Documents and Settings*userid*\Local Settings\Temp\configApp.log
- Documents and Settings*userid*\Local Settings\Temp\configAppErr.log

On UNIX platforms

- /tmp/installApp.log
- /tmp/installAppErr.log
- /tmp/configApp.log
- /tmp/configAppErr.log

Logs used by the InstallShield GUI when installing and uninstalling DB2 on Windows are:

When installing

- Documents and Settings*userid*\Local Settings\Temp\DB2setup.log
- Documents and Settings*userid*\Local Settings\Temp\db2wi.log
- Documents and Settings*userid*\Local Settings\Temp\db2inst.log
- Documents and Settings*userid*\Local Settings\Temp\db2insterr.log

When uninstalling

- Documents and Settings*userid*\Local Settings\Temp\DB2remove.log
- Documents and Settings*userid*\Local Settings\Temp\db2uninst.log
- Documents and Settings*userid*\Local Settings\Temp\db2uninsterr.log
- Documents and Settings*userid*\Local Settings\Temp\db2uninsttrc.log

© Copyright IBM Corp. 1998, 2003

Failed installation

Another reason for an installation failure is lack of disk space. IBM Tivoli Directory Server attempts to verify that there is enough space and generates messages if the required disk space is not found, but sometimes the InstallShield GUI cannot progress far enough to issue a message. Before installing, make sure you have the recommended free disk space. All platforms use temporary space, and in addition, UNIX platforms use the `/var` directory. When installation is first run, the JVM is installed to the installation directory, so be sure that your installation destination directory has enough space.

Recovering from a failed installation

The first step to recovering from a failed installation is to run the InstallShield Uninstall GUI to clean up any registry entries that might have been made by the installation process. If you do not run the InstallShield Uninstall GUI, the InstallShield GUI might fail the next time you try to use it to install IBM Tivoli Directory Server. See the following sections for information organized by operating system. See "Uninstalling using the InstallShield GUI" on page 100 for information about uninstalling using the InstallShield GUI.

When installing on UNIX platforms, the InstallShield GUI uses the native packages (for example, AIX installp files, Solaris .pkg files, or RPM files) to install IBM Tivoli Directory Server. Because of this, you will see these packages when you run the platform commands (such as `rpm -qa` on the Linux operating system) to query what is installed. Even though you can use the platform commands (such as `rpm -e`) to uninstall, you **must** use the InstallShield GUI to uninstall so that the InstallShield Registry is cleaned up.

Windows operating system

On Windows platforms:

1. Uninstall IBM Tivoli Directory Server using the InstallShield GUI. See "Windows platforms" on page 100 for information.
2. Remove the IBM Tivoli Directory Server installation directory. The default directory is C:\Program Files\IBM\LDAP.
3. Correct any other problems listed in the ldapinst.log file.
4. Use **regedit** to remove the LDAP entry in the registry: HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP
5. Remove the following environment variables:

   LDAPHome=C:\Program Files\IBM\LDAP
   LIBPATH=C:\Program Files\IBM\LDAP\JAVA
   LOCPATH=C:\Program Files\IBM\LDAP\bin\locale
   NLSPATH=C:\Program Files\IBM\LDAP\NLS\MSG\%L\%N
   Path=C:\Program Files\IBM\LDAP\bin
   TISDIR=C:\Program Files\IBM\LDAP

   Note: The InstallShield GUI also sets the LANG environment variable (LANG=enus1252); however, because other programs might use this environment variable, it is not in the list of environment variables to remove.

AIX operating system

On the AIX operating system:

1. Uninstall IBM Tivoli Directory Server using the InstallShield GUI. See "UNIX platforms" on page 100 for information.

2. Type the following at a command prompt:
```
lslpp -l |grep -i ldap
```
3. If any packages that were installed by IBM Tivoli Directory Server were left on the system, use **installp** to uninstall them, as follows:
```
installp -u packagename
```
4. Remove the /usr/ldap directory.
5. Correct any other problems that were listed in the ldapinst.log.

   Note: AIX operating system installation generates an additional log called installp_isje.log. You must review this log to determine if there were failures in the **installp** commands issued by the InstallShield GUI.

Linux operating system

On the Linux operating system:

1. Uninstall IBM Tivoli Directory Server using the InstallShield GUI. See "UNIX platforms" on page 100 for information.
2. Type the following at a command prompt:
```
rpm -qa | grep -i ldap
```
   If any packages that were installed by IBM Tivoli Directory Server were left on the system, use the **rpm** command to uninstall them. For example:
```
rpm -ev  packagenames
```
3. If an **rpm** command hangs, try running the command with the **noscripts** option:
```
rpm -ev  --noscripts packagenames
```
4. Remove the /usr/ldap directory.
5. Correct any other problems that were listed in the ldapinst.log file.

Solaris operating system

On the Solaris operating system:

1. Uninstall IBM Tivoli Directory Server using the InstallShield GUI. See "UNIX platforms" on page 100 for information.
2. Type the following at a command prompt:
```
pkginfo | grep -i ldap
```
3. If any packages that were installed by IBM Tivoli Directory Server were left on the system, use **pkgrm** to uninstall them:
```
pkgrm packagenames
```
   Note: If you encounter problems removing these packages, try to remove the directories containing the packages from /var/sadm/pkg
4. Remove the /opt/IBMldapc and /opt/IBMldaps directories, and any other directories left from the installation, such as a language directory.
5. Correct any other problems that were listed in the ldapinst.log.

Configuration

The following sections contain troubleshooting information about configuration.

DB2 license file expired

If you see the following message during the configuration of the database
```
Failed to start database manager for instance: ldapdb2
```

you might have a problem with your electronic DB2 license. To verify this, type the following at the command prompt:

```
db2start
```

If your license is correct, you see the message:

```
SQL1063N DB2START processing was successful.
```

Otherwise, you see a message indicating that your license has expired or will expire in some number of days.

If there is a problem with your electronic DB2 license, one of the following situations might be the cause:

- You have a demonstration license.
  1. To upgrade your DB2 product from a demonstration license to a product license, copy the license file from the DB2 CD to the system where DB2 is installed; you do not need to reinstall DB2.

     Note: Your Proof of Entitlement and License Information booklets identify the products for which you are licensed.
  2. After you have a valid license on the system, run the following command to activate the license:

     ```
     db2licm -a license_filename
     ```
- You have purchased a different DB2 product.

  If you install a DB2 product as Try-and-Buy, and you buy a different DB2 product, you must uninstall the Try-and-Buy product and then install the new one that you have purchased. Type the following at a command prompt to upgrade your DB2 license:

  ```
  db2licm -a license_filename
  ```

Note: *license_filename* is the name of the license file; for example, db2udbee.lic.

Translated titles might truncate in Configuration Tool

In the Configuration Tool, titles in the pop-up windows might truncate depending upon the language. If this problem occurs, depending on your display, you can resize the the window accordingly.

Interrupting Configuration Tool database tasks causes an incorrect status for the files

If you are using the Configuration Tool to configure, unconfigure, import, export, backup, restore, or optimize a database and the process is interrupted by, for example, a segmentation fault, the status of the files is returned incorrectly. When you try to restart the process, the message

```
Task is already running.
```

is displayed. This is because the status output for the process is monitored through files in the $LDAPHOME/tmp folder that were not deleted when the process was interrupted.

To restart the interrupted process, you must first manually delete the following two files:

- $LDAPHOME/tmp/ldapcfg.dat
- $LDAPHOME/tmp/ldapcfg.stat

Java failure when configuring an existing instance and database

If you are using United Linux 1.0, Red Hat Advanced Server 2.1, or AIX with DB2 v8.1 and you are configuring an existing instance and database, a Java failure might occur after the configuration is completed. This failure, however, can be ignored. The instance and database are successfully configured. For example, if you issued the command:

```
ldapcfg -a <myuserID> -w <mypassword> -d <mydatabase> -l /home/<myuserID>
```

the following message might be displayed after the completion of the configuration process:

```
IBM Directory Server Configuration complete.
Unexpected exception has occurred:
ReportedExceptionCode = b, at ExceptionAddress = 74736574
        ACCESS_VIOLATION occured outside Interpreter and JITed code
        ExecMode = EXECMODE_BYTECODE
        stackpointer=0xbffc7370
Writing Java core file ....
Written Java core to /var/ldap/javacore9151.1035571351.txt
Abort
```

Error when starting the Configuration Tool on AIX

The following error might occur when you start the Configuration Tool on AIX:

```
# ldapxcfg exec(): 0509-036 Cannot load program ldapxcfg
                         because of the following errors:
         0509-022 Cannot load module /usr/ldap/lib/libdbadmin.a.
         0509-150   Dependent module /usr/ldap/lib/libdb2.a(shr_64.o) could not .
         0509-152   Member shr_64.o is not found in archive
```

If this error occurs, check the following:

- You have the correct version of DB2 (DB2 8.1, FixPak 2, 64-bit)
- You have 64-bit hardware. See "Verifying that AIX hardware is 64-bit" on page 115
- You are running a 64-bit kernel. See "Verifying that the AIX kernel is 64-bit" on page 115
- You migrated your database to 64-bit. See "Migration from IBM Directory Server version 4.1 or 5.1 for AIX installations" on page 37

Configuration programs terminate on AIX

If the configuration programs (**ldapcfg**, **ldapxcfg**, and **ldapucfg**) terminate immediately when you start them, check the LIBPATH. If the *jre*/bin/classic directory of a JVM other than the one provided with IBM Tivoli Directory Server comes before the %LDAPHOME%/java/bin/classic directory, do one of the following:

- Remove the extraneous JVMs from the LIBPATH.
- Place the %LDAPHOME%/java/bin/classic directory in front of the other JVM directories in the LIBPATH.

DB2 does not configure properly

Note: Before configuring the database, be sure that the environment variable DB2COMM is **not** set.

If a failure occurs during database configuration, usually one of the following is the cause:

- The user ID was not set up correctly. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for information.
- The permissions for the user ID are not correct. See "Before you configure: creating the DB2 database owner and database instance owner" on page 85 for information.
- Remnants of a previous database or DB2 instance with the name you specified for the database are present on the system.
- There is not enough space in the location you specified.

Check to see if there are problems with any of these items, and then try to configure again after you fix the problem.

Note: If you use the Configuration Tool to configure and configuration fails, the Configuration Tool does some cleanup, and this can sometimes fix the problem. If you do not find any of the problems in the list, try configuring again.

Database performance is poor

For detailed information about improving performance (including information about buffer pools), see the *IBM Tivoli Directory Server Version 5.2 Performance Tuning Guide*.

Server does not start after making changes to configuration files attributes

The attributes defined in IBM Tivoli Directory Server configuration files are significant to only the first 18 characters. Names longer than 18 characters are truncated to meet the DB2 restriction.

If you want to index the attribute, the limit is further restricted to 16 characters. If you add attributes longer than 18 characters, the server might not start. For additional information, see the Server Administration helps under **Reference**, Directory Schema.

Transaction log is full

The following messages might be displayed at IBM Tivoli Directory Server startup if the schema defines too many attributes:

```
SQL0965C The transaction log for the database is full
SQLSTATE=57011 slapd unable to start because all backends failed to configure
```

You might need to increase the DB2 transaction log sizes by typing:

```
db2 update db cfg for ldaptest using logprimary X
db2 update db cfg for ldaptest using logsecond X
```

where *X* is greater than what is currently defined.

Configuration Tool

The following sections apply to the Configuration Tool.

Some keyboard commands fail on Browse windows

You might not be able to use the Space, Enter or arrow keys on the keyboard to view the contents of the **Look in** menu on a **Browse** window. To work around this problem, press Alt+Down Arrow to display the **Look in** menu, and use the arrow keys to select a drive.

NullPointer exception when exiting the Configuration Tool

If you exit the Configuration Tool after entering an invalid database name, a NullPointer exception occurs in the command window where the **ldapxcfg** command was executed. The exception does not affect the configuration process.

Debugging

The following sections provide debugging information.

Error opening slapd.cat on Windows

On Windows systems, you might receive an error message that includes the following:

```
Error opening slapd.cat
Plugin of type DATABASE is successfully loaded from C:/Program Files/IBM/LDAP/bi
n/libback-config.dll.
Error opening rdbm.cat
```

If this occurs, check the NLSPATH environment variable. The installation program sets the NLSPATH environment variable as a system environment variable. However, if the system also has the NLSPATH variable set as a user environment variable , the user NLSPATH environment variable overrides the system setting.

To correct this, you can append the NLSPATH information from the system environment variable to the information in the user environment variable.

Logging on to the Web Administration Tool console on Internet Explorer

On Windows, Web Administration errors occur if all the following conditions exist:

- The Web Administration Tool is installed locally
- The Web Administration Tool runs on a locally installed version of Microsoft Internet Explorer
- The Web Administration Tool uses the locally installed embedded version of WebSphere Application Server - Express
- An IP address or hostname is part of the URL used to access the Web Administration Tool

If these conditions exist on your computer, avoid errors by using localhost instead of an IP address or hostname when logging on to the Web Administration GUI console.

For example, open an Internet Explorer Web browser and type the following in the **Address** field:

```
http://localhost:9080/IDSWebApp/IDSjsp/Login.jsp
```

Corruption of data entered in Web Administration Tool

If data that you enter in non-English languages in the Web Administration Tool is corrupted, do the following:

On the embedded version of WebSphere Application Server - Express

Edit the server.xml file in the following directory:

```
WAS_home/appsrv/config/cells/DefaultNode/nodes/DefaultNode/servers/server1
```

Add the text shown in bold to the stanza as shown:

```
<processDefinition xmi:type="processexec:JavaProcessDef"
   xmi:id="JavaProcessDef_1"
   executableName="${JAVA_HOME}/bin/java"
   executableTarget="com.ibm.ws.runtime.WsServer"
   executableTargetKind="JAVA_CLASS"
   workingDirectory="${USER_INSTALL_ROOT}">
<execution xmi:id="ProcessExecution_1" processPriority="20" runAsUser=""
   runAsGroup=""/>
<monitoringPolicy xmi:id="MonitoringPolicy_1" pingInterval="60"
   maximumStartupAttempts="3" pingTimeout="300" autoRestart="true"
   nodeRestartState="STOPPED" />
<ioRedirect xmi:id="OutputRedirect_1"
   stdoutFilename="${SERVER_LOG_ROOT}/native_stdout.log"
   stderrFilename="${SERVER_LOG_ROOT}/native_stderr.log"/>
<jvmEntries xmi:id="JavaVirtualMachine_1" classpath="" bootClasspath=""
   verboseModeClass="false" verboseModeGarbageCollection="false"
   verboseModeJNI="false" initialHeapSize="0"
   maximumHeapSize="256" runHProf="false" hprofArguments=""
   debugMode="false" debugArgs="-Djava.compiler=NONE -Xdebug -Xnoagent
   -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
   genericJvmArguments="">
<systemProperties xmi:id="Property_10"
   name="client.encoding.override" value="UTF-8" required="false"/>
</jvmEntries>
```

On WebSphere Application Server

On the WebSphere Administrative Console tree:

- Select **Servers**.
- Select **Application Server**.
- Select the server you want; for example, `server1`.
- Click **Process Definition**.
- Click **Java Virtual Machine**.
- Click **Custom Properties**.
- Click the appropriate button for making a new property.
- In the **Name** field, type `client.encoding.override`.
- In the **Value** column, type `UTF-8`.
- Click **Apply**.
- Stop and restart the WebSphere Application Server.

DB2 errors logged

In addition to the ibmslapd.log file, which can be accessed through the Web Administration Tool, DB2 errors are logged in the db2cli.log file. Both files are located in the var subdirectory of the IBM Tivoli Directory Server installation directory on Windows platforms.

Note: The var subdirectory might include other DB2 files.

Server errors are logged in the \var\ibmslapd.log file.

DB2 errors are logged in the \var\db2cli.log file.

Server debug mode

If the error logs do not provide enough information to resolve a problem, you can run the server in a special debug mode that generates very detailed information. The server executable **ibmslapd** must be run from a command prompt to enable debug output. The syntax is as follows:

```
ldtrc on
ibmslapd -h bitmask
```

where the specified bitmask value determines which categories of debug output are generated.

The ldtrc program controls the LDAP Trace Facility. For example, the following ldtrc search:

```
ldapsearch -l 60 -h ddejesus -D "o=IBM_US, c=US" -w
secret -b "ou=Austin, o=IBM_US, c=US" "cn=Cindy Corn"
```

might return server output similar to the following:

```
Connection received from 9.53.95.251 on socket 540.
  86366975       704 usec SQLAllocStmt() => 0
  86367557        73 usec SQLBindParameter() => 0
  86367974        33 usec SQLBindParameter() => 0
  86435508        52 usec SQLFetch => 0
  86436039        49 usec SQLGetData => 0
  86436835       454 usec SQLFreeStmt => 0
  86458726       629 usec SQLAllocStmt() => 0
  86459708       561 usec SQLPrepare(SELECT distinct
DB2ADMIN.LDAP_ENTRY.EID FROM DB2ADMIN.LDA
P_ENTRY,DB2ADMIN.LDAP_DESC  WHERE
(DB2ADMIN.LDAP_ENTRY.EID=DB2ADMIN.LDAP_DESC.DEID
AND DB2ADMIN.LDAP_DESC.AEID=?) AND  DB2ADMIN.LDAP_ENTRY.EID
IN (SELECT EID FROM DB2ADMIN.CN WHERE CN_T= ?)) => 0
```

Another way to enable server debug mode is to activate the server trace from startup. To do this, set the ibm-slapdStartupTraceEnabled environment variable to TRUE in the server configuration file. There are configuration options for setting the level and routing the output to a file.

The following example shows the ibm-slapdStartupTraceEnabled option set to true:

```
dn: cn=Configuration
cn: Configuration
ibm-slapdACLAccess: true
ibm-slapdAdminDN: cn=root
ibm-slapdAdminGroupEnabled: true
ibm-slapdAdminPW:
       >14T/+cmSHfFQ8nKkYschiuw421kXnH6F0VP6NjfwlkBq3w1E65QBWCVczbcrt
        E++R7AEnKYFiBQFGBNJ0qYVny6ZmcXsFvhsniFKEpYFwLvLmxYFEpFuZkoPnju
        ttmTMMMogn/MKty288T8mc8JWMB1L+3gWWiW26y<
ibm-slapdDerefAliases: always
ibm-slapdErrorLog: /var/ibmslapd.log
ibm-slapdMaxPendingChangesDisplayed: 200
ibm-slapdPort: 389
#ibm-slapdPwEncryption must be one of none/imask/crypt/sha
ibm-slapdPwEncryption: imask
ibm-slapdServerId: 3a98a5d7-35c2-4c2b-a789-7255204efd4a
ibm-slapdSizeLimit: 500
ibm-slapdStartupTraceEnabled: true
ibm-slapdSupportedWebAdmVersion: 2.0
#ibm-slapdSysLogLevel must be one of l/m/h (l=terse, h=verbose)
ibm-slapdSysLogLevel: m
ibm-slapdTimeLimit: 900
ibm-slapdTraceMessageLevel: 0xFFFF
```

```
ibm-slapdTraceMessageLog: /var/ibmslapd.trace.log
ibm-slapdVersion: 5.2
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdTop
```

You must run the `ldtrc on` command before the server is started.

The server can be traced dynamically.

To activate the LDAP Trace Facility, use `ldtrc on` or, from any machine where IBM Tivoli Directory Server is installed, issue the following command:

```
ldaptrace -h <hostname> -d <adminDN> -w <adminpassword> -l on
```

Some other useful commands include:

- To start tracing IBM Tivoli Directory Server:
  ```
  ldaptrace -h <hostname> -d <adminDN> -w <adminpassword> -l on -t start
  ```
- To stop tracing IBM Tivoli Directory Server:
  ```
  ldaptrace -h <hostname> -d <adminDN> -w <adminpassword> -l on -t stop
  ```
- To turn off the LDAP Trace Facility:
  ```
  ldaptrace -h <hostname> -d <adminDN> -w <adminpassword> -l off
  ```
- To show the state of the LDAP Trace Facility:
  ```
  ldaptrace -h <hostname> -d <adminDN> -w <adminpassword> -l info
  ```
- To display the ldaptrace command usage information:
  ```
  ldaptrace -?
  ```

See Table 3 for descriptions of debug categories.

Table 3. Debug categories

Hex	Decimal	Value	Description
0x0001	1	LDAP_DEBUG_TRACE	Entry and exit from routines
0x0002	2	LDAP_DEBUG_PACKETS	Packet activity
0x0004	4	LDAP_DEBUG_ARGS	Data arguments from requests
0x0008	8	LDAP_DEBUG_CONNS	Connection activity
0x0010	16	LDAP_DEBUG_BER	Encoding and decoding of data
0x0020	32	LDAP_DEBUG_FILTER	Search filters
0x0040	64	LDAP_DEBUG_MESSAGE	Messaging subsystem activities and events
0x0080	128	LDAP_DEBUG_ACL	Access Control List activities
0x0100	256	LDAP_DEBUG_STATS	Operational statistics
0x0200	512	LDAP_DEBUG_THREAD	Threading statistics
0x0400	1024	LDAP_DEBUG_REPL	Replication statistics
0x0800	2048	LDAP_DEBUG_PARSE	Parsing activities
0x1000	4096	LDAP_DEBUG_PERFORMANCE	Relational backend performance statistics

Table 3. Debug categories (continued)

Hex	Decimal	Value	Description
0x1000	8192	LDAP_DEBUG_RDBM	Relational backend activities (RDBM)
0x4000	16384	LDAP_DEBUG_REFERRAL	Referral activities
0x8000	32768	LDAP_DEBUG_ERROR	Error conditions
0xffff	65535	ALL	
0x7fffffff	2147483647	LDAP_DEBUG_ANY	All levels of debug

For example, specifying a bitmask value of 65535 turns on full debug output and generates the most complete information.

When you are finished, issue the following command at a command prompt:

```
ldtrc off
```

It is recommended that you contact IBM Service for assistance with interpreting the debug output and resolving the problem.

Verifying that AIX hardware is 64-bit

The server on AIX requires 64-bit hardware. To verify that your AIX hardware is 64-bit, run the following command:

```
bootinfo -y
```

If the command returns `32`, your hardware is 32-bit.

In addition, if you type the command `lsattr -El proc0`, the output of the command returns the type of processor for your server. If you have any of the following, you have 64-bit hardware: RS64 I, II, III, IV, POWER3, POWER3 II or POWER4.

Verifying that the AIX kernel is 64-bit

To verify that you have the 64 bit kernel (/usr/lib/boot/unix_64) installed and running, run the following command:

```
bootinfo -K
```

In addition, if you type the command `lsattr -El proc0`, the output of the command returns the type of processor for your server. If you have any of the following, you have 64-bit hardware: RS64 I, II, III, IV, POWER3, POWER3 II or POWER4.

Note: If the hardware is 32-bit, then you can only have a 32-bit kernel. You cannot have a 64-bit kernel. If the hardware is 64-bit, then you can have either a 32 or 64-bit kernel. Go to http://www.ibm.com/support/docview.wss?uid=isg1hintsTips0214#4 for detailed information.

Error on AIX 5.1 when running db2start

The following error might occur when you try to run **db2start**:

```
0509-130 Symbol resolution failed for /usr/lib/threads/libc.a(aio.o)
because:
        0509-136   Symbol kaio_rdwr (number 0) is not exported from
                   dependent module /unix.
        0509-136   Symbol listio (number 1) is not exported from
```

```
              dependent module /unix.
0509-136   Symbol acancel (number 2) is not exported from
              dependent module /unix.
0509-136   Symbol iosuspend (number 3) is not exported from
              dependent module /unix.
0509-136   Symbol aio_nwait (number 4) is not exported from
              dependent module /unix.
0509-192 Examine .loader section symbols with the
         'dump -Tv' command.
```

If this occurs on AIX 5.1, you have asynchronous I/O turned off.

To turn on asynchronous I/O:

1. Run **smitty chgaio** and set **STATE to be configured at system restart** from **defined** to **available**.
2. Press Enter.
3. Do **one** of the following:
   - Restart your system.
   - Run **smitty aio** and move the cursor to **Configure defined Asynchronous I/O**. Then press Enter.

The **db2start** command now works.

Error when starting the embedded version of WebSphere Application Server - Express on AIX

Starting the embedded version of WebSphere Application Server - Express on AIX (**startServer.sh server1**) might not work because port 9090 is already being used. See the *installpath*/logs/server1 directory for the actual log files. Usually the SystemErr.log and SystemOut.log files are the most helpful, although the other logs might have some useful information.

To change the port number for the embedded version of WebSphere Application Server - Express from 9090 to an unused port (for example, 9091) which is the port used on AIX machines. Edit the *installpath*/config/cells/DefaultNode/virtualhosts.xml file and change 9090 to 9091. Make the same change in the

```
installpath/config/cells/DefaultNode/nodes/DefaultNode/servers/server1/server.xml
```

file.

Notes:

1. This path does have two subdirectories called DefaultNode.
2. *installpath* is the directory where the embedded version of WebSphere Application Server - Express is installed.

Migration

During migration, the following log files might be created.

On UNIX platforms:

Errors that occurred during schema migration are logged in the /tmp/migrate.errors file.

Detailed messages concerning schema migration are logged in the /tmp/migrate52.log file.

On Windows platforms:

The migration process uses the following log files:

Errors that occur during schema migration are logged in the *install directory*\tmp\migrate.errors file.

Detailed messages received during schema migration are logged in the *install directory*\tmp\migrate52.log file.

Standard out from execution of migrate52.bat is in the *install directory*\tmp\migrate52StdOut.log file.

Standard error from execution of migrate52.bat is in the *install directory*\tmp\migrate52StdErr.log file.

Other log files are:

- Documents and settings*userid*\local settings\temp\ldapaddcfg.log
- Documents and settings*userid*\local settings\temp\ldapaddmaster.log
- Documents and settings*userid*\local settings\temp\ldaprmdbcfg.log
- Documents and settings*userid*\local settings\temp\ldaprmchlog.log
- Documents and settings*userid*\local settings\temp\ldapaddibmldapver.log
- Documents and settings*userid*\local settings\temp\ldapaddpeer.log
- Documents and settings*userid*\local settings\temp\ldapaddreplica.log

Web browser problems

The following information might be helpful if you encounter problems with your Web browser.

Microsoft Internet Explorer

If you have problems with Microsoft Internet Explorer, try making the following changes to the cache setup:

- Click **Tools —> Internet Options**, and select **General**. Then click **Settings**. Under **Check for newer versions of stored pages**, click **Every visit to the page**.
- If you are getting unpredictable results using the browser, the cache might be storing pages with errors. On the General folder page, click **Delete files** and **Clear History** to clear the cache. Use these options as often as necessary.
- Shutting down and restarting the browser can also repair some intermittent problems.

Appendix A. Database configuration planning

Before configuring and populating your database, determine:

What type of data you are going to store in the directory

Decide what sort of schema you need to support the type of data you want to keep in your directory. A standard set of attribute-type definitions and object-class definitions is included with the directory server. Before you begin adding entries to the directory, you might want to add new attribute-type and object-class definitions that are customized to your data.

Note: You can make schema additions after the directory is already populated with data, but schema changes might require you to unload and reload your data.

Which code page you are going to use

Decide whether to create your database using the local code page or using the Universal Character Set (UTF-8). Selecting the local code page enables IBM Tivoli Directory Server applications and users to get search results as expected for the collation sequence of the native language. Using UTF-8 enables the storing of any UTF-8 character data in the directory. IBM Tivoli Directory Server clients running anywhere in the world (in any UTF-8 supported language) can access and search the directory. In many cases, however, the client might have limited ability to properly display the results retrieved from the directory in a particular language or character set. See Appendix H, "UTF-8 support", on page 135 for more information.

Note: If you want to use language tags, the database must be a UTF-8 database.

How you want to structure your directory data

An IBM Directory is stored in a hierarchical tree structure. The names of entries in the directory are based on their relative position within the tree structure. It is important to define some logical organization to the directory. A logical organization makes it easier for clients to determine which branch of the tree contains the information they are trying to locate. If you are storing data about the people in an organization, it is easy to map the structure of the organization onto the structure of the directory. If you are storing descriptions of applications, machine configuration data, or customer data, it might take more planning to decide how to structure your directory.

Your data security requirements

See the Secure Sockets Layer information in the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for information about how your data is secured.

How you want to allocate access permissions

See the access control lists information in the *IBM Tivoli Directory Server version 5.2 Administration Guide* for information about using access permissions.

© Copyright IBM Corp. 1998, 2003

Appendix B. Support for additional locales on UNIX platforms

On some UNIX systems, depending on your locale settings, server messages might be generated in English, rather than in the language associated with the locale. For example, if your locale is set to de_DE, German messages are displayed. However, if your locale is set to de_CH, English messages are displayed.

If this occurs, you can create symbolic links to select a language for messages on AIX, Linux, or HP-UX.

For example, on AIX or Linux, to select German messages for a locale in Switzerland, (de_CH), create links by typing the following at a command prompt:

```
cd /usr/lib/nls/msg
ln -sf de_DE/diradm.cat de_CH/diradm.cat
ln -sf de_DE/ldapc.cat de_Ch/ldapc.cat
ln -sf de_DE/ldapcp.cat de_Ch/ldapcp.cat
ln -sf de_DE/ldapprod.cat de_Ch/ldapprod.cat
ln -sf de_DE/ldaputil.cat de_Ch/ldaputil.cat
ln -sf de_DE/ldcf.cat de_Ch/ldcf.cat
ln -sf de_DE/rdbm.cat de_Ch/rdbm.cat
ln -sf de_DE/slapd.cat de_Ch/slapd.cat
ln -sf de_DE/webutil.cat de_Ch/webutil.cat
```

On HP-UX, for example, to enable the Spanish translation for a locale in Mexico, (es_MX), create links by typing the following at a command prompt:

```
cd /usr/lib/nls/msg
ln -sf es_ES.iso88591/diradm.cat es_MX.iso88591/diradm.cat
ln -sf es_ES.iso88591/ldapc.cat es_MX.iso88591/ldapc.cat
ln -sf es_ES.iso88591/ldapcp.cat es_MX.iso88591/ldapcp.cat
ln -sf es_ES.iso88591/ldapprod.cat es_MX.iso88591/ldapprod.cat
ln -sf es_ES.iso88591/ldaputil.cat es_MX.iso88591/ldaputil.cat
ln -sf es_ES.iso88591/ldcf.cat es_MX.iso88591/ldcf.cat
ln -sf es_ES.iso88591/rdbm.cat es_MX.iso88591/rdbm.cat
ln -sf es_ES.iso88591/slapd.cat es_MX.iso88591/slapd.cat
ln -sf es_ES.iso88591/webutil.cat es_MX.iso88591/webutil.cat
```

© Copyright IBM Corp. 1998, 2003

Appendix C. Migrating replication servers

Use the information in this section before migration if you have replication servers in your installation.

If you are migrating from IBM Directory Server 5.1, no migration is required for replication.

When you install an IBM Tivoli Directory Server 5.2 server over an existing IBM Directory Server 4.1 server, the server updates the `cn=Master Server` entry in the ibmslapd.conf file. Auxiliary class **ibm-slapdPendingMigration** is added to the `cn=Master Server` entry to indicate that replication migration should be done during the initial startup of the server. On some platforms the ibmslapd.conf file is updated when migration scripts are run. These migration scripts **must** be run after installation, but before the initial start of the server following installation.

The following example shows the `cn=Master Server` entry in the ibmslapd.conf file; the information in **bold type** is added during migration. (For Windows, migration occurs during installation.)

```
dn: cn=Master Server, cn=configuration
objectclass: top
objectclass: ibm-slapdReplication
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPendingMigration
ibm-slapdMigrationInfo:  4.1 REPLICA
cn: Master Server
ibm-slapdMasterDN: cn=master
ibm-slapdMasterPW: masterpass2
ibm-slapdMasterReferral: ldap://mymaster.mycompany.com
```

The value of the **ibm-slapdMigrationInfo** attribute indicates what type of server is being migrated. The following are valid values for this attribute:

4.1 REPLICA	Read-only replica
4.1 MASTER	Read-write master
4.1 PEER	Read-write peer replica

If your server configuration file did not contain an entry for `cn=MasterServer`, the migration process adds the following:

```
dn: cn=Master Server, cn=configuration
objectclass: top
objectclass: ibm-slapdReplication
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPendingMigration
ibm-slapdMigrationInfo:  4.1 MASTER
```

Replication migration is a one-time operation and occurs only during the initial start of the server, and only when the **ibm-slapdPendingMigration** auxiliary class is configured for the `cn=Master Server` entry. It is possible to restore a 4.1 version of the database and manually add the **ibm-slapdPendingMigration** class to the

© Copyright IBM Corp. 1998, 2003

`cn=Master Server` entry to migrate replication-related information separately. All replication topology configuration and all unfinished replication activity will be migrated in the following ways:

- If this is a read-only replica server, then an ibm-replicationContext, ibm-replicaGroup, and ibm-replicaSubentry will be created for each suffix configured for the server except for the CN=SCHEMA, CN=LOCALHOST, and CN=PWDPOLICY suffixes.
- If this is a peer or master server, then an ibm-replicationContext, ibm-replicaGroup, and ibm-replicaSubentry will be created only if replicaObject entries exist under the cn=localhost subtree.
- For peer and master servers, all replicaObject entries under the cn=localhost subtree will be migrated to ibm-replicationAgreement, and ibm-replicationCredentials directory entries.
- For master and peer servers with replicaObject entries, convert currently outstanding replication data and status in the CHANGE and PROGRESS tables to the newly defined IBM Tivoli Directory Server 5.1 REPLCHANGE, REPLSTATUS, and REPLCSTAT tables.
- When replication is successfully completed, the **ibm-slapdPendingMigration** auxiliary class will be removed from the `cn=Master Server` entry in the ibmslapd.conf file, and the obsolete CHANGE and PROGRESS tables will be deleted from the database.

After running any migration scripts, which are required for some platforms, the first startup of IBM Tivoli Directory Server 5.2 automatically handles all replication topology and data migration for a master or peer server. However, it is always a good idea to make a backup of your directory data to prevent data loss in case of an unforeseen failure.

Note: After migration, if you notice discrepancies between the previous replication topology and the newly migrated topology, use the **ldapdiff** tool to fix the problem. See the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for information about using **ldapdiff**.

Appendix D. Installing, configuring, and uninstalling the embedded version of WebSphere Application Server - Express

To use the Web Administration Tool, an application server is required. The embedded version of WebSphere Application Server - Express, v5.0.2 is provided with IBM Tivoli Directory Server 5.2 as an application server.

If you use the InstallShield GUI to install the Web Administration Tool, you can select the embedded version of WebSphere Application Server - Express for installation. In this case, configuration is also done automatically.

If you use native installation methods, you can install and configure the embedded version of WebSphere Application Server - Express manually. If you already have the embedded version of WebSphere Application Server - Express v 5.0.2 installed, you must configure manually before you can use the Web Administration Tool.

Manually installing and configuring the embedded version of WebSphere Application Server - Express

Installing the embedded version of WebSphere Application Server - Express

To manually install the embedded version of WebSphere Application Server - Express, use the following procedure:

1. After you download and unzip (or untar) the IBM Tivoli Directory Server zip or tar file, change directories to the directory where you expanded the file.
2. Type the following command at a command prompt:
   - On Windows platforms:
     ```
     install.bat -installRoot installpath\appsrv -hostName localhost
     ```
   - On UNIX platforms:
     ```
     install.sh -installRoot installpath/appsrv -hostName localhost
     ```

   where
   - *installpath* is the directory where you unzipped or untarred the file.
   - appsrv is the subdirectory where you are installing the embedded version of WebSphere Application Server - Express. By convention, appsrv is the directory used, though you can change this subdirectory if necessary.

   After installing the Web Administration Tool, copy the Web Administration Tool to the embedded version of WebSphere Application Server - Express directory by using the following commands:
   ```
   mkdir installpath/appsrv/installableApps/
   cp installpath/idstools/IDSWebApp.war installpath/appsrv/installableApps/
   ```

Installing the Web Administration Tool into the embedded version of WebSphere Application Server - Express

Install the Web Administration Tool into the embedded version of WebSphere Application Server - Express by using the following command:

© Copyright IBM Corp. 1998, 2003

- On Windows systems:

```
"installpath\appsrv\bin\wsadmin.bat" -conntype NONE -c "$AdminApp
     install {installpath\appsrv\installableApps\IDSWebApp.war}
     {-configroot \"installpath\appsrv/config\"
     -node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
     -contextroot \"IDSWebApp\"}"
```

  Note: Type the command on one line.
- On UNIX systems:

```
installpath/appsrv/bin/wsadmin.sh -conntype NONE -c "\$AdminApp
     install {installpath/appsrv/installableApps/IDSWebApp.war}
     {-configroot \"installpath/appsrv/config\"
     -node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
     -contextroot \"IDSWebApp\"}"
```

Notes:

1. If you install the Web Administration Tool and the embedded version of WebSphere Application Server - Express through the InstallShield GUI, these commands are run automatically.
2. If you plan to use the Web Administration Tool in a non-English language, see "Corruption of data entered in Web Administration Tool" on page 111.

Uninstalling the Web Administration Tool from the embedded version of WebSphere Application Server - Express

To uninstall the Web Administration Tool from the embedded version of WebSphere Application Server - Express manually:

1. Be sure that the application server is started. See "Starting the application server to use the Web Administration Tool" on page 97 for instructions.
2. Type the following at a command prompt to uninstall the Web Administration Tool:
   - On Windows platforms:

     ```
     WASPath\bin\wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
     ```
   - On UNIX platforms:

     ```
     WASPath/bin/wsadmin.sh -conntype NONE -c "\$AdminApp uninstall IDSWebApp.war"
     ```

   where *WASPath* is the path where you installed the embedded version of WebSphere Application Server - Express.

Default ports for the embedded version of WebSphere Application Server - Express

The embedded version of WebSphere Application Server - Express uses four default port settings:

- Http Transport (port 1): 9080
- Http Transport (port 2): 9443
- Bootstrap/rmi port: 2809
- Soap connector port: 8880

If a conflict exists with another application using one or more of these default ports, you can use a text editor to change from the default ports to unused ports.

Http Transport port 1

Find the line containing the port number 9080 in the following files and replace the 9080 with the port number that you want:

$*WASHOME*\config\cells\DefaultNode\nodes\DefaultNode\servers\server1\server.xml
$*WASHOME*\config\cells\DefaultNode\virtualhosts.xml

where *WASHOME* is the directory where the embedded version of WebSphere Application Server - Express is installed.

Http Transport port 2

Find the line containing the port number 9443 in the following files and replace the 9443 with the port number that you want:

$*WASHOME*\config\cells\DefaultNode\nodes\DefaultNode\servers\server1\server.xml
$*WASHOME*\config\cells\DefaultNode\virtualhosts.xml

where *WASHOME* is the directory where the embedded version of WebSphere Application Server - Express is installed.

Bootstrap/rmi port

Find the line containing the port number 2809 in the following file and replace the 2809 with the port number that you want:

`$WASHOME\config\cells\DefaultNode\nodes\DefaultNode\serverindex.html`

where *WASHOME* is the directory where the embedded version of WebSphere Application Server - Express is installed.

Soap connector port

Find the line containing the port number 8880 in the following file and replace the 8880 with the port number that you want:

`$WASHOME\config\cells\DefaultNode\nodes\DefaultNode\serverindex.html`

where *WASHOME* is the directory where the embedded version of WebSphere Application Server - Express is installed.

Using HTTPS for the embedded version of WebSphere Application Server - Express Version V5.0.2

The embedded version of WebSphere Application Server - Express, V5.0.2 comes with HTTPS set up by default on port 9443. To use HTTPS, you must change your login URL to the following:

https://<*hostname*>:9443/IDSWebApp/IDSjsp/Login.jsp

For non-HTTPS connections, continue to use the URL:

http://<*hostname*>:9080/IDSWebApp/IDSjsp/Login.jsp

Additionally, if you want to change the application server's SSL certificate, you can create new key and trust store database files for the embedded version of WebSphere Application Server - Express to use. By default, the key and trust store database files are separate and are located in the <*WASHOME*>/etc directory. These files are named **DummyServerKeyFile.jks** and **DummyServerTrustFile.jks** respectively.

After you have created your new jks files, you can change the key and trust store database files that WAS uses by modifying the following items (highlighted in **bold**) in the <*WASHOME*>/config/cells/DefaultNode/security.xml file to use your new file names, passwords, and file formats:

```
<repertoire xmi:id="SSLConfig_1" alias="DefaultSSLSettings">
  <setting xmi:id="DefaultSSLSettings"
     keyFileName="${USER_INSTALL_ROOT}/etc/DummyServerKeyFile.jks"
     keyFilePassword="WebAS" keyFileFormat="JKS"
     trustFileName="${USER_INSTALL_ROOT}/etc/DummyServerTrustFile.jks"
     trustFilePassword="WebAS" trustFileFormat="JKS"
     clientAuthentication="false" securityLevel="HIGH"
     enableCryptoHardwareSupport="false">
      <cryptoHardware xmi:id="CryptoHardwareToken_1" tokenType=""
         libraryFile="" password=""/>
      <properties xmi:id="Property_4" name="com.ibm.ssl.protocol" value="SSLv3"/>
      <properties xmi:id="Property_5" name="com.ibm.ssl.contextProvider"
         value="IBMJSSE"/>
  </setting>
</repertoire>
```

Appendix E. Installing the Web Administration Tool into WebSphere

IBM Tivoli Directory Server 5.2 provides the embedded version of WebSphere Application Server - Express version 5.0.2 as an application server for the Web Administration Tool. However, you can also use WebSphere version 5.0 or higher as an application server for the Web Administration Tool. If you use WebSphere, you must install the Web Administration Tool into WebSphere. Use the following instructions as a guide:

1. Install WebSphere, using the installation information provided with it.
2. Install the Web Administration Tool using either the InstallShield GUI or the installation utility for your operating system. The file containing the Web Administration Tool is named IDSWebApp.war, and it is in the idstools subdirectory of the installation directory you specified during installation.
3. Install the Web Administration Tool application into WebSphere, using the information provided with WebSphere. For example, if you use the Administrative Console, on the Install New Application window, set the **Local path** to *installdirectory*/idstools/IDSWebApp.war, and the **Context root** to /IDSWebApp.

   installdirectory is the directory you specified when installing the Web Administration Tool.
4. Start the Web Administration Tool (for example, through the Administrative Console).
5. From a Web browser, type the following address:
   `http://localhost:9080/IDSWebApp/IDSjsp/Login.jsp`

   The IBM Tivoli Directory Server Web Administration login page window is displayed.

   Note: This address works only if you are running the browser on the computer on which the Web Administration Tool is installed. If the Web Administration Tool is installed on a different computer, replace `localhost` with the hostname or IP address of the computer where the Web Administration Tool is installed.

Note: If you plan to use the Web Administration Tool in a non-English language, see "Corruption of data entered in Web Administration Tool" on page 111.

Appendix F. Installing and configuring DSML

Directory Services Markup Language (DSML) is installed as a .zip file named DSML.zip in the *installpath*/idstools (or *installpath*\idstools for Windows systems) directory when you install the Web Administration Tool. After you unzip the DSML.zip file, documentation files are available that tell you how to install, configure, and use DSML. These files are:

DSMLReadme.txt
Describes the files in the package and tells you how to install and configure DSML.

dsml.pdf
Describes how to use DSML. This file is in PDF format.

dsml.htm
Describes how to use DSML, in HTML format.

Appendix G. Loading a sample database

Use the following procedure to load a sample database.

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left.
2. In the Manage suffixes window, in the **SuffixDN** field, type `o=ibm,c=us`. This is the suffix DN that will hold the sample data. Because the sample data is part of the suffix **o=ibm,c=us**, this is the suffix DN you must add.
3. Click **Add**.
4. Click **OK**.

   Note: When you click **Add**, the suffix is added to the list in the **Current suffix DNs** box; however, the suffix is not actually added until you click **OK**.
5. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
6. In the Import LDIF data window on the right, in the **Path and LDIF file name** field, type one of the following:
   - `install_dir\examples\sample.ldif` on Windows systems
   - `install_dir/examples/sample.ldif` on UNIX systems

   Alternatively, you can click **Browse** to locate the file. *install_dir* is the directory where you installed IBM Tivoli Directory Server.
7. Click **Standard import**.
8. Click **Import**.

Note: As an alternative, you can use:
- The **ldapcfg** command to add the suffix: `ldapcfg -s "o=ibm,c=us"`
- The **ldif2db** utility to import the data. For example, `ldif2db -i install_dir\examples\sample.ldif`

9. After processing is complete, go to a command prompt and type `ibmslapd` to start the server.

   Messages are displayed while the server is starting. The following message is displayed if the server starts successfully:

   ```
   IBM Tivoli Directory, Version 5.2 Server started.
   ```

You have verified that the sample database is loaded correctly and that the installation is successful.

Use the instructions in "Starting the Web Administration Tool" on page 97 to start the Web Administration Tool if you installed it. See the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for information about using the Web Administration Tool and using the server.

© Copyright IBM Corp. 1998, 2003

Appendix H. UTF-8 support

IBM Tivoli Directory Server supports a wide variety of national language characters through the UTF-8 (UCS Transformation Format) character set. As specified for the LDAP Version 3 protocol, all character data that is passed between an LDAP client and a server is in UTF-8. Consequently, the directory server can be configured to store any national language characters that can be represented in UTF-8. The limitations on what types of characters can be stored and searched for are determined by how the database is created. The database character set can be specified as UTF-8 or it can be set to use the server system's local character set (based on the locale, language, and code page environment).

If you specify UTF-8, you can store any UTF-8 character data in the directory. LDAP clients running anywhere in the world (in any UTF-8 supported language) can access and search the directory. In many cases, however, the client has limited ability to properly display the results retrieved from the directory in a particular language/character set. There is also a performance advantage to using a UTF-8 database because no data conversion is required when storing data to or retrieving data from the database.

Note: If you want to use language tags, the database must be a UTF-8 database.

Why choose anything other than UTF-8?

A UTF-8 database has a fixed collation sequence. That sequence is the binary order of the UTF-8 characters. It is not possible to do language-sensitive collation with a UTF-8 database.

If it is important to your LDAP applications or users to get results for a search using an ordering filter (for example, "name >= SMITH") or any search specifying the control to sort the results as they would expect for their native language, then UTF-8 might not be the appropriate character set for their directory database. In that instance, the LDAP server system and all client systems should run using the same character set and locale. For example, an LDAP server running in a Spanish locale with a database created using that locale returns results of searches based on character ordering, as Spanish-language clients would expect. This configuration does limit your directory user community to a single end-user character set and collation sequence.

Server utilities

Manual creation of an LDIF file containing UTF-8 values is difficult. To simplify this process, a charset extension to the LDIF format is supported. This extension allows an Internet Assigned Numbers Authority (IANA) character set name to be specified in the header of the LDIF file (along with the version number). A limited set of the IANA character sets are supported.

Examples

You can use the optional charset tag so that the server utilities automatically convert from the specified character set to UTF-8 as in the following example:

© Copyright IBM Corp. 1998, 2003

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

In this instance, all values following an attribute name and a single colon are translated from the ISO-8859-1 character set to UTF-8. Values following an attribute name and a double colon (such as description:: V2hhdCBhIGNhcm...) should be base 64-encoded, and are expected to be either binary or UTF-8 character strings. Values read from a file, such as the jpegPhoto attribute specified by the URL in the example above, are also expected to be either binary or UTF-8. No translation from the specified "charset" to UTF-8 is done on those values.

In this example of an LDIF file without the charset tag, content is expected to be in UTF-8:

```
# IBM IBM Directorysample LDIF file
#
# The suffix "o=IBM, c=US" should be defined before attempting to load
# this data.

 version: 1

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Mary Smith, ou=Austin, o=IBM, c=US
```

This same file could be used without the version: 1 header information, as in previous releases of IBM Tivoli Directory Server:

```
# IBM IBM Directorysample LDIF file
#
#The suffix "o=IBM, c=US" should be defined before attempting to load
#this data.

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Supported IANA character sets

IBM Tivoli Directory Server supports the Internet Assigned Number Authority (IANA) character set names by platform, as shown in the following table. These are the character set names that can be specified in an LDIF file or using the C-client interface to identify the character set of input data to be used with the directory.

Table 4. Supported IANA character sets by platform

Character	Locale				DB2 Code Page	
Set Name	**Linux, Linux for S/390®, HP-UX**	**NT**	**AIX**	**Solaris**	**UNIX**	**NT**
ISO-8859-1	X	X	X	X	819	1252
ISO-8859-2	X	X	X	X	912	1250
ISO-8859-5	X	X	X	X	915	1251
ISO-8859-6	X	X	X	n/a	1089	1256
ISO-8859-7	X	X	X	n/a	813	1253
ISO-8859-8	X	X	X	n/a	916	1255
ISO-8859-9	X	X	X	n/a	920	1254
IBM437	n/a	X	n/a	n/a	437	437
IBM850	n/a	X	X	n/a	850	850
IBM852	n/a	X	n/a	n/a	852	852
IBM857	n/a	X	n/a	n/a	857	857
IBM862	n/a	X	n/a	n/a	862	862
IBM864	n/a	X	n/a	n/a	864	864
IBM866	n/a	X	n/a	n/a	866	866
IBM869	n/a	X	n/a	n/a	869	869
TIS-620	n/a	X	X	n/a	874	874
EUC-JP	X	n/a	X	X	954	n/a
EUC-KR	n/a	n/a	X	X	970	n/a
EUC-CN	n/a	n/a	X	X	1383	n/a
EUC-TW	n/a	n/a	X	X	964	n/a
Shift-JIS	X	X	X	X	932	943
KSC	n/a	X	n/a	n/a	n/a	949
GBK	n/a	X	X	n/a	1386	1386
Big5	n/a	X	X	X	950	950

Appendix I. Setting up GSKit to support CMS key databases

To set up GSKit to support Conversational Monitor System (CMS) key databases, complete the following procedure before starting the iKeyman GUI:

1. Be sure that you have installed GSKit 7a.
2. Install the IBM JRE or JDK 1.4.1 or an equivalent JRE or JDK.
3. Set JAVA_HOME to point to the directory where Java 1.4.1 was installed. For example:
   - On Windows, set JAVA_HOME=c:\Program Files\IBM\Java14.
   - On AIX, export JAVA_HOME=/usr/ldap/java.
4. On AIX, create a link from /usr/ldap/jre to /usr/ldap/java by typing the following at a command prompt:
   ```
   ln -s /usr/ldap/java /usr/ldap/jre
   ```
5. Remove the ibmjsse.jar, gskikm.jar (if it exists) and ibmjcaprovider.jar files from your JAVA_HOME\jre\lib\ext directory on Windows. This directory is JAVA_HOME/lib/ext (/usr/ldap/java/lib/ext) on AIX.
6. Be sure that the JAVA_HOME\jre\ (/usr/ldap/java/ on AIX) directory has the following JAR files:
   - lib/ext/ibmjceprovider.jar
   - lib/ext/ibmpkcs.jar
   - lib/ibmjcefw.jar
   - lib/ext/ibmjcefips.jar (optional to support FIPS)
   - lib/security/local_policy.jar
   - lib/security/US_export_policy.jar
   - lib/ibmpkcs11.jar

   On Solaris, JDK 1.4 requires the user to have jurisdiction policy files. Due to the import restrictions for some countries, the jurisdiction policy files distributed with the J2SDK version 1.4.1 software have built-in restrictions on the available cryptographic strength. The Solaris installation requires jurisdiction policy files that contain no restrictions on cryptographic strength.

   For more information about jurisdiction policy files, see the following Web site:

   http://java.sun.com/products/jce/index-14.html

   To download, go to the following Web site:

   http://java.sun.com/j2se/1.4/download.html#docs

   Note: GSKit has provided the jar files shown and ibmpkcs11.jar under *GSKit_installation_path*\classes\jre\lib\ext for your convenience. It is up to each individual product to decide whether to ship these JSSE jar files in the product. The following are the GSKit recommendations:
   - A product should ship whatever JSSE jar files it used for system testing with the product.
   - If your existing Java installation's JSSE jar files are later than those required by GSKit, no action is required.

    - If your existing Java installation's JSSE jar files are older than those required by GSKit, your should replace your old JSSE jar files with the GSKit jar files. GSKit iKeyman will work with the old JSSE jar files. However, some iKeyman functions might fail due to known bug fixes that are not included in your JDK installation.
7. GSKit users must register both IBM CMS and IBM JCE service providers as follows:

   Update the JAVA_HOME/jre/lib/security/java.security file to add both IBM CMS and IBM JCE providers after the Sun provider. For example:

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=com.ibm.spi.IBMCMSProvider
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   ```

   A sample java.security file can be found in *GSKit_Installation_path*\classes\gsk_java.security.

   To enable FIPS operation, update the JAVA_HOME/jre/lib/security/java.security file to add IBMCMS, IBMJCE, and IBMJCEFIPS providers after the Sun provider. Be sure that the IBMJCEFIPS provider was registered at a higher priority than IBMJCE. For example:

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=com.ibm.spi.IBMCMSProvider
   security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.4=com.ibm.crypto.provider.IBMJCE
   ```
8. This step is optional. If you are a JSSE user and use JSSE to access cryptographic hardware, install the ibmpkcs11.jar file in the JAVA_HOME\jre\lib\ext directory and follow the instructions in *GSKit_Installation_path*/classes/native/native-support.zip to set up the cryptographic hardware DLLs.

   Note: You could also find the ibmpkcs11.jar file in the JSSE package released after August 5, 2002. To register an IBMPKCS11 service provider, the following example updates the JAVA_HOME/jre/lib/security/java.security file:

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.crypto.pkcs11.provider.IBMPKCS11
   ```

Appendix J. Configuring the database in a location other than /home when /home is an NFS mount

On UNIX systems, if you use NFS automount, you must configure everything manually to create the database in a location other than /home. Performing manual configuration in this situation also avoids the problem of the **ldapcfg** command trying to write to /home.

Notes:

1. The following steps assume that you want to set up a database where the instance owner is ldapdb2, DB2 instance is ldapdb2, and database name is ldapdb2.
2. It is strongly recommended to save a copy of any system file before editing it.

1. Create a group named dbsysadm for the database administrators:

   ```
   groupadd [-g <gid>] dbsysadm
   ```

   Note: The **groupadd** command on some Linux distributions requires that the group ID number (gid) be specified using the **-g** *<gid>* syntax. Type

   ```
   cat /etc/group
   ```

   to find an available group ID number. Red Hat automatically assigns the next available gid if the **-g** option is not specified.
2. Add users root and ldap to the dbsysadm group:

   ```
   usermod -G dbsysadm root
   usermod -G dbsysadm ldap
   ```
3. Create a user account (ldapdb2) for the DB2 instance:

   ```
   useradd -g dbsysadm -m ldapdb2
   ```
4. Set the password for the user account (ldapdb2):

   ```
   passwd ldapdb2
   ```

   Enter the new password when prompted. Record your password for future reference.
5. Create the database instance:

   ```
   <LDAPHOME>/db2/instance/db2icrt -u ldapdb2 ldapdb2
   ```

   where *<LDAPHOME>* is:
   - AIX, Linux operating systems- /usr/ldap
   - Solaris operating systems - /opt/IBMldaps
   - HP-UX operating systems- /usr/IBMldap
6. Log in as the database user ID:

   ```
   su - ldapdb2
   ```
7. Start the database manager:

   ```
   db2start
   ```
8. Create the database under the instance:

   ```
   db2 create db ldapdb2 on <location> using codeset UTF-8 territory US
   ```

   Note: If you omit the `using codeset UTF-8 territory US` the database is created in the local code page. However, using the local code page does affect performance. The database requires at least 80Mb of free space available on the filesystem. Use **df -k** to verify this before creating the database.

9. Enable multi-page file allocation:

   ```
   db2empfa ldapdb2
   ```

   Note: This is a performance enhancement, and cannot be undone after being run.

10. Update some of the DB2 tuning variables:

    ```
    db2 update db cfg for <databasename> using <parm> <newvalue>
    DB2 Parameter Minimum value allowed
    APPLHEAPSZ 2048
    PCKCACHESZ 360
    SORTHEAP   256
    ```

    For example:

    ```
    db2 update db cfg for ldapdb2 using APPLHEAPSZ 1280
    ```

11. The database is fully configured; you can update the configuration file to use this database. In <*LDAPHOME*>etc/ibmslapd.conf, in the following stanza:

    ```
    dn: cn=Directory,cn=RDBM Backends,cn=IBM SecureWay,cn=Schemas,cn=Configuration
    objectclass: top
    objectclass: ibm-slapdRdbmBackend
    cn: Directory
    ibm-slapdPlugin:  database /bin/libback-rdbm.dll rdbm_backend_init
    ibm-slapdDbConnections:  15
    ibm-slapdSuffix:  cn=localhost
    ibm-slapdReadOnly:  FALSE
    ```

    Add the following lines:

    ```
    ibm-slapdDbInstance: ldapdb2
    ibm-slapdDbAlias: ldapdb2b
    ibm-slapdDbUserId: ldapdb2
    ibm-slapdDbUserPw: <user pw>
    ibm-slapdDbLocation: <user defined location>
    ```

    The resulting stanza is:

    ```
    dn: cn=Directory,cn=RDBM Backends,cn=IBM SecureWay,cn=Schemas,cn=Configuration
    objectclass: top
    objectclass: ibm-slapdRdbmBackend
    cn: Directory
    ibm-slapdPlugin:  database /bin/libback-rdbm.dll rdbm_backend_init
    ibm-slapdDbInstance: ldapdb2
    ibm-slapdDbAlias: ldapdb2b
    ibm-slapdDbUserId: ldapdb2
    ibm-slapdDbUserPw: <user pw>
    ibm-slapdDbLocation: <user defined location>
    ibm-slapdDbConnections:  15
    ibm-slapdSuffix:  cn=localhost
    ibm-slapdReadOnly:  FALSE
    ```

12. If you used a UTF-8 datastore as described in step 8 on page 141, in the stanza: dn: cn=Front End, cn=Configuration, you must uncomment the line:

    ```
    #ibm-slapdSetEnv: DB2CP=1208
    ```

The database is ready for the Directory server to use. The first startup takes longer because the server must create its own tablespaces and bufferpools.

Appendix K. IBM Tivoli Directory Server configuration schema

This appendix describes the Directory Information Tree (DIT) and the attributes that are used to configure the ibmslapd.conf file. In some previous releases, the directory configuration settings were stored in a proprietary format in the configuration file. Starting with the Version 3.2 release, the directory settings are stored using the LDIF format in the configuration file.

The configuration file was renamed from slapd32.conf to ibmslapd.conf in the 5.1 release. The schema used by the configuration file is also now available. Attribute types can be found in the v3.config.at file, and object classes are in the v3.config.oc file. Attributes can be modified using the **ldapmodify** command. See the *IBM Tivoli Directory Server Version 5.2 Administration Guide* for information about the **ldapmodify** command.

Directory Information Tree

cn=Configuration

- cn=Admin
- cn=AdminGroup
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server
- cn=Referral
- cn=Schema
  - cn=IBM Directory
    - cn=Config Backends
      - cn=ConfigDB
    - cn=RDBM Backends
      - cn=Directory
      - cn=ChangeLog
    - cn=LDCF Backends
      - cn=SchemaDB
- cn=SSL
  - cn=CRL
- cn=Transaction
- cn=Digest
- cn=admin audit
- cn=Audit
- cn=Connection Management

cn=Configuration

DN cn=Configuration

Description

This is the top-level entry in the configuration DIT. It holds data of global

© Copyright IBM Corp. 1998, 2003

interest to the server, although in practice it also contains miscellaneous items. Every attribute in the this entry comes from the first section (global stanza) of ibmslapd.conf.

Number
1 (required)

Object Class
ibm-slapdTop

Mandatory Attributes
- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdDerefAliases
- objectClass

Optional Attributes
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion
- ibm-slapdAdminGroupEnabled
- ibm-slapdStartupTraceEnabled
- ibm-slapdTraceMessageLog
- ibm-slapdTraceMessageLevel

cn=Admin

DN cn=Admin, cn=Configuration

Description
Global configuration settings for IBM Admin Daemon

Number
1 (required)

Object Class
ibm-slapdAdmin

Mandatory Attributes
- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Optional Attributes
- ibm-slapdSecurePort

cn=AdminGroup

DN cn=<id>, cn=AdminGroup, cn=Configuration

Description
A user belonging to the Administration Group. Must be an entry under the cn=AdminGroup, cn=Configuration subtree.

Number
0 (optional) Needed only if you want administrative group members.

Object Class
ibm-slapdAdminGroupMember

Mandatory Attributes
- ibm-slapdAdminDN
- ibm-slapdAdminPW

Optional Attributes
- ibm-slapdKrbAdminDN
- ibm-slapdDigestAdminUser

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Description
Global event notification settings for IBM Tivoli Directory Server 5.1

Number
0 or 1 (optional; needed only if you want to enable event notification)

Object Class
ibm-slapdEventNotification

Mandatory Attributes
- cn
- ibm-slapdEnableEventNotification
- objectClass

Optional Attributes
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Description
Global environment settings that the server applies at startup.

Number
0 or 1 (optional)

Object Class
ibm-slapdFrontEnd

Mandatory Attributes
- cn
- objectClass

Optional Attributes

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Description
Global Kerberos authentication settings for IBM Tivoli Directory Server 5.2.

Number
0 or 1 (optional)

Object Class
ibm-slapdKerberos

Mandatory Attributes

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Optional Attributes

- None

cn=Master Server

DN cn=Master Server, cn=Configuration

Description
When configuring a replica, this entry holds the bind credentials and referral URL of the master server.

Number
0 or 1 (optional)

Object Class
ibm-slapdReplication

Mandatory Attributes

- cn
- ibm-slapdMasterPW (Mandatory if not using Kerberos authentication.)
- objectClass

Optional Attributes

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Optional if using Kerberos authentication.)
- ibm-slapdMasterReferral

cn=Referral

DN cn=Referral, cn=Configuration

Description
This entry contains all the referral entries from the first section (global stanza) of ibmslapd.conf. If there are no referrals (there are none by default), this entry is optional.

Number
0 or 1 (optional)

Object Class
ibm-slapdReferral

Mandatory Attributes
- cn
- ibm-slapdReferral
- objectClass

Optional Attributes
- None

cn=Schemas

DN cn=Schemas, cn=Configuration

Description
This entry serves as a container for the schemas. This entry is not really necessary because the schemas can be distinguished by the object class ibm-slapdSchema. It is included to improve the readability of the DIT.

Only one schema entry is currently allowed: cn=IBM Directory.

Number
1 (required)

Object Class
Container

Mandatory Attributes
- cn
- objectClass

Optional Attributes
- None

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the schema configuration data from the first section (global stanza) of ibmslapd.conf. It also serves as a container for all the backends that use the schema. Multiple schemas are not supported, but if they were, then there would be one ibm-slapdSchema entry per schema.

Note that multiple schemas are assumed to be incompatible. Therefore, a backend can be associated with a single schema only.

Number
1 (required)

Object Class
ibm-slapdSchema

Mandatory Attributes

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Optional Attributes

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry serves as a container for the Config backends.

Number
1 (required)

Object Class
Container

Mandatory Attributes

- cn
- objectClass

Optional Attributes
None

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
Configuration backend for IBM Tivoli Directory Server server configuration

Number
0 - n (optional)

Object Class
ibm-slapdConfigBackend

Mandatory Attributes

- cn
- ibm-slapdSuffix
- ibm-slapdPlugin
- objectClass

Optional Attributes

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry serves as a container for the RDBM backends. It effectively replaces the database rdbm line from ibmslapd.conf by identifying all sub-entries as DB2 backends. This entry is not really necessary because the RDBM backends can be distinguished by object class ibm-slapdRdbmBackend. It is included to improve the readability of the DIT.

Number
0 or 1 (optional)

Object Class
Container

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- None

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the database configuration settings for the default RDBM database backend.

Although multiple backends with arbitrary names can be created, the Server Administration assumes that "cn=Directory" is the main directory backend, and that "cn=Change Log" is the optional changelog backend. Only the suffixes displayed in "cn=Directory" are configurable through the Server Administration (except for the changelog suffix, which is set transparently by enabling changelog).

Number
0 - n (optional)

Object Class
ibm-slapdRdbmBackend

Mandatory Attributes

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- objectClass

Optional Attributes

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdChangeLogMaxAge
- ibm-slapdCLIErrors

- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdLanguageTagsEnabled

Note: If you are using **ibm-slapdUseProcessIdPw**, you must modify the schema to make **ibm-slapdDbUserPW** optional.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the database configuration settings for the change log backend.

Number
0 - n (optional)

Object Class
ibm-slapdRdbmBackend

Mandatory Attributes
- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- objectClass

Optional Attributes
- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation

- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdLanguageTagsEnabled

Note: If you are using **ibm-slapdUseProcessIdPw**, you must modify the schema to make **ibm-slapdDbUserPW** optional.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry serves as a container for the LDCF backends. It effectively replaces the database ldcf line from ibmslapd.conf by identifying all sub-entries as LDCF backends. This entry is not really necessary because the LDCF backends can be distinguished by the object class ibm-slapdLdcfBackend. It is included to improve the readability of the DIT.

Number
1 (required)

Object Class
Container

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the database configuration data from the ldcf database section of ibmslapd.conf.

Number
1 (required)

Object Class
ibm-slapdLdcfBackend

Mandatory Attributes

- cn

- objectClass

Optional Attributes

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Description
Global SSL connection settings for IBM Tivoli Directory Server 5.2.

Number
0 or 1 (optional)

Object Class
ibm-slapdSSL

Mandatory Attributes

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Optional Attributes

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Note: **ibm-slapdSslCipherSpecs** is now deprecated. Use **ibm-slapdSslCipherSpec** instead. If you use **ibm-slapdSslCipherSpecs**, the server will convert to the supported attribute.

- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFilePW
- ibm-slapdSslFIPsModeEnabled

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Description
This entry contains certificate revocation list data from the first section (global stanza) of ibmslapd.conf. It is needed only if "ibm-slapdSslAuth = serverclientauth" in the cn=SSL entry and the client certificates have been issued for CRL validation.

Number
0 or 1 (optional)

Object Class
ibm-slapdCRL

Mandatory Attributes

- cn
- ibm-slapdLdapCrlHost

- ibm-slapdLdapCrlPort
- objectClass

Optional Attributes

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Description

Specifies Global transaction support settings. Transaction support is provided using the plugin:

Windows 2000, or Windows NT operating system:

```
extendedop /bin/libtranext.dll tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

AIX:

```
extendedop /lib/libtranext.a tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Solaris operating system:

```
extendedop /lib/libtranext.so tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

The server (**slapd**) loads this plug-in automatically at startup if **ibm-slapdTransactionEnable** = **TRUE**. The plug-in does not need to be explicitly added to **ibmslapd.conf**.

Number

0 or 1 (optional; required only if you want to use transactions.)

Object Class

ibm-slapdTransaction

Mandatory Attributes

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Optional Attributes

- None

cn=Digest

DN cn = Digest, cn = Configuration

Description

Global configuration entries for the DIGEST-MD5 SASL bind mechanism.

Number

0 or 1 (optional)

Object Class
ibm-slapdDigest

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- ibm-slapdDigestRealm
- ibm-slapdDigestAttr
- ibm-slapdDigestAdminUser

cn=admin audit

DN cn = admin audit, cn = Configuration

Description
Audit service configuration for the server.

Number
0 or 1 (optional)

Object Class
ibm-auditConfig

Mandatory Attributes

- cn

Optional Attributes

- ibm-audit
- ibm-auditAdd
- ibm-auditBind
- ibm-auditDelete
- ibm-auditExtOpEvent
- ibm-auditFailedOpOnly
- ibm-auditLog
- ibm-auditModify
- ibm-auditModifyDN
- ibm-auditSearch
- ibm-auditUnbind
- ibm-auditVersion
- ibm-auditExtOp

cn=Audit

DN cn = admin audit, cn = Configuration

Description
Audit service configuration for the admin daemon.

Number
0 or 1 (optional)

Object Class
ibm-auditConfig

Mandatory Attributes

- cn

Optional Attributes

- ibm-audit
- ibm-auditAdd
- ibm-auditBind
- ibm-auditDelete
- ibm-auditExtOpEvent
- ibm-auditFailedOpOnly
- ibm-auditLog
- ibm-auditModify
- ibm-auditModifyDN
- ibm-auditSearch
- ibm-auditUnbind
- ibm-auditVersion
- ibm-auditExtOp

cn=Connection Management

DN cn=Connection Management, cn=Front End, cn=Configuration

Description
Global connection settings

Number
0 or 1 (optional)

Object Class
ibm-slapdConnectionManagement

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- ibm-slapdEThreadEnable
- ibm-slapdAllowAnon
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdAllReapingThreshold
- ibm-slapdIdleTimeOut
- ibm-slapdWriteTimeout
- ibm-slapdESizeThreshold
- ibm-slapdETimeThreshold
- ibm-slapdEThreadActivate

Attributes

- cn
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN

- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxAge
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdSslKeyRingFilePW
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword

- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslFIPsModeEnabled
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdStartupTraceEnabled
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTraceMessageLevel
- ibm-slapdTraceMessageLog
- ibm-slapdTransactionEnable

- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

cn

Description
This is the X.500 common Name attribute, which contains a name of an object.

Syntax
Directory string

Maximum Length
256

Value Multi-valued

ibm-slapdACLCache

Description
Controls whether or not the server caches ACL information.

- If set to TRUE, the server caches ACL information.
- If set to FALSE, the server does not cache ACL information.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdACLCacheSize

Description
Maximum number of entries to keep in the ACL Cache.

Default
25000

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdAdminDN

Description
The administrator bind DN for IBM Tivoli Directory Server server.

Default
cn=root

Syntax
DN

Maximum Length
Unlimited

Value Single-valued

ibm-slapdAdminGroupEnabled

Description
Specifies whether the Administrative Group is currently enabled. If set to TRUE, the server will allow users in the administrative group to log in.

Default
FALSE

Syntax
Boolean

Maximum Length
128

Value Single-valued

ibm-slapdAdminPW

Description
The administrator bind password for IBM Tivoli Directory Server server.

Default
secret

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdAllowAnon

Description
Specifies if anonymous binds are allowed.

Default
True

Syntax
Boolean

Maximum Length
128

Value Single-valued

ibm-slapdAllReapingThreshold

Description
Specifies a number of connections to maintain in the server before connection management is activated.

Default
1200

Syntax
Directory string with case-exact matching.

Maximum Length
1024

Value Single-valued

ibm-slapdAnonReapingThreshold

Description
Specifies a number of connections to maintain in the server before connection management of anonymous connections is activated.

Default
0

Syntax
Directory string with case-exact matching.

Maximum Length
1024

Value Single-valued

ibm-slapdBoundReapingThreshold

Description
Specifies a number of connections to maintain in the server before connection management of anonymous and bound connections is activated.

Default
1100

Syntax
Directory string with case-exact matching.

Maximum Length
1024

Value Single-valued

ibm-slapdBulkloadErrors

Description
File path or device on ibmslapd host machine to which bulkload error messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory (for example, /tmp/bulkload.errors = D:\Program Files\IBM\ldap\tmp\bulkload.errors).

Default
/var/bulkload.log

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdCachedAttribute

Description
Contains the names of the attributes to be cached in the attribute cache, one attribute name per value.

Default
None

Syntax
Directory string

Maximum Length
256

Value Multi-valued

ibm-slapdCachedAttributeSize

Description
Amount of memory, in bytes, that can be used by the attribute cache. A value of 0 indicates not use an attribute cache.

Default
0

Syntax
Integer

Maximum Length
11

Value Single-valued.

ibm-slapdChangeLogMaxAge

Description
Specifies the maximum age of changelog entries, in hours, allowed in the associated backend. Each changelog backend has its own ibm-slapdChangeLogMaxAge attribute. If the attribute is undefined or out of range (negative), it defaults to 0. Can be between 0 (no limit) and 2,147,483,647.

Default
0

Syntax
Signed Integer

Maximum Length
11

Value Single-valued

ibm-slapdChangeLogMaxEntries

Description
This attribute is used by a changelog plug-in to specify the maximum number of changelog entries allowed in the RDBM database. Each changelog has its own changeLogMaxEntries attribute.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647 (32-bit, signed integer)
```

Default
0

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdCLIErrors

Description
File path or device on ibmslapd host machine to which CLI error messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the install directory (for example, /tmp/cli.errors = D:\Program Files\IBM\ldap\tmp\cli.errors).

Default
/var/db2cli.log

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdConcurrentRW

Description
Setting this attribute to TRUE allows searches to proceed simultaneously with updates. It allows for 'dirty reads', that is, results that might not be consistent with the committed state of the database.

Attention: This attribute is deprecated.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdDB2CP

Description
Specifies the code page of the directory database. 1208 is the code page for UTF-8 databases.

Syntax
Directory string with case-exact matching

Maximum Length
11

Value Single-valued

ibm-slapdDBAlias

Description
The DB2 database alias.

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

ibm-slapdDbConnections

Description
Specify the number of DB2 connections the server will dedicate to the DB2 backend. The value must be between 5 & 50 (inclusive).

Note: ODBCCONS environment variable overrides the value of this directive.

If ibm-slapdDbConnections (or ODBCCONS) is less than 5 or greater than 50, the server will use 5 or 50 respectively. One additional connection will be created for replication (even if no replication is defined). 2 additional connections will be created for the change log (if change log is enabled).

Default
15

Syntax
Integer

Maximum Length
50

Value Single-valued

ibm-slapdDbInstance

Description
Specifies the DB2 database instance for this backend.

Default
ldapdb2

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

Note: All ibm-slapdRdbmBackend objects must use the same ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW and DB2 character set.

ibm-slapdDbLocation

Description
The file system path where the backend database is located. On UNIX, this is usually the home directory of the DB2 instance owner (for example, /home/ldapdb2). On Windows, it is a drive (for example, D:).

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdDbName

Description
Specifies the DB2 database name for this backend.

Default
ldapdb2

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

ibm-slapdDbUserID

Description
Specifies the user name with which to bind to the DB2 database for this backend.

Default
ldapdb2

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

Note: All ibm-slapdRdbmBackend objects must use the same ibm-slapdDbInstance ibm-slapdDbUserID, ibm-slapdDbUserPW and DB2 character set.

ibm-slapdDbUserPW

Description
Specifies the user password with which to bind to the DB2 database for this backend. The password can be plain text or imask encrypted.

Default
ldapdb2

Syntax
Binary

Maximum Length
128

Value Single-valued

Note: All ibm-slapdRdbmBackend objects must use the same ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW and DB2 character set.

ibm-slapdDerefAliases

Description
Maximum alias dereferencing level on search requests, regardless of any derefAliases that may have been specified on the client requests. Allowed values are **never**, **find**, **search** and **always**.

Default
always

Syntax
Directory string

Maximum Length
6

Value Single-valued

ibm-slapdDigestAdminUser

Description
Specifies the Digest MD5 User Name of the LDAP administrator or administrative group member. Used when MD5 Digest authentication is used to authenticate an administrator.

Default
None

Syntax
Directory string

Maximum Length
512

Value Single-valued

ibm-slapdDigestAttr

Description
Overrides the default DIGEST-MD5 username attribute. The name of the attribute to use for DIGEST-MD5 SASL bind username lookup. If the value is not specified, the server uses uid.

Default
If not specified, the server uses uid.

Syntax
Directory string.

Maximum Length
64

Value Single-valued

ibm-slapdDigestRealm

Description
Overrides the default DIGEST-MD5 realm. A string that can enable users to know which username and password to use, in case they might have different ones for different servers. Conceptually, it is the name of a collection of accounts that might include the users account. This string should contain at least the name of the host performing the authentication and might additionally indicate the collection of users who might have access. An example might be `registered_users@gotham.news.example.com`. If the attribute is not specified, the server uses the fully qualified hostname of the server.

Default
The fully qualified hostname of the server

Syntax
Directory string.

Maximum Length
1024

Value Single-valued

ibm-slapdEnableEventNotification

Description
Specifies whether to enable Event Notification. It must be set to either TRUE or FALSE.

If set to FALSE, the server rejects all client requests to register event notifications with the extended result LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdEntryCacheSize

Description
Maximum number of entries to keep in the entry cache.

Default
25000

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdErrorLog

Description
Specifies the file path or device on the IBM Tivoli Directory Server server machine to which error messages are written. On Windows 2000 or Windows NT operating systems, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory, that is /tmp/slapd.errors = c:\Program Files\IBM\ldap\var\ibmslapd.log.

Default
/var/ibmslapd.log

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdESizeThreshold

Description
Specifies the number of work items on the work queue before the Emergency thread is activated.

Default
50

Syntax
Integer

Maximum Length
1024

Value Single-valued

ibm-slapdEThreadActivate

Description
Specifies which conditions will activate the Emergency Thread. Must be set to one of the following values:

S	Size only
T	Time only
SOT	Size or time
SAT	Size and time

Default
SAT

Syntax
String

Maximum Length
1024

Value Single-valued

ibm-slapdEThreadEnable

Description
Specifies if the Emergency Thread is active.

Default
True

Syntax
Boolean

Maximum Length
1024

Value Single-valued

ibm-slapdETimeThreshold

Description
Specifies the amount of time in minutes between items removed from the work queue before the Emergency thread is activated.

Default
5

Syntax
Integer

Maximum Length
1024

Value Single-valued

ibm-slapdFilterCacheBypassLimit

Description
Search filters that match more than this number of entries will not be added to the Search Filter cache. Because the list of entry IDs that matched the filter are included in this cache, this setting helps to limit memory use. A value of 0 indicates no limit.

Default
100

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdFilterCacheSize

Description
Specifies the maximum number of entries to keep in the Search Filter Cache.

Default
25000

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdIdleTimeOut

Description
Maximum time to keep an LDAP connection open when there is no activity on the connection. The idle time for an LDAP connection is the time (in seconds) between the last activity on the connection and the current time. If the connection has expired, based on the idle time being greater than the value of this attribute, the LDAP server will clean up and end the LDAP connection, making it available for other incoming requests.

Default
300

Syntax
Integer

Length
11

Count Single

Usage Directory operation

User Modify
Yes

Access Class
Critical

Required
No

ibm-slapdIncludeSchema

Description
Specifies a file path on the IBM Tivoli Directory Server server machine containing schema definitions. On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and a leading slash not preceded by a drive letter (D:) is assumed to be rooted at the installation directory; that is, /etc/V3.system.at = D:\Program Files\IBM\ldap\etc\V3.system.at.

Default

/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Multi-valued

ibm-slapdSslKeyRingFilePW

Description
Specifies the password associated with the LDAP server's SSL key database file, as specified on the ibm-slapdSslKeyRingFile parameter. If the LDAP server's key database file has an associated password stash file, then the ibm-slapdSslKeyRingFilePW parameter can be omitted or set to `ibm-slapdSslKeyRingFilePW = none`.

Note: The password stash file must be located in the same directory as the key database file and it must have the same file name as the key database file, but with an extension of .sth instead of .kdb.

Default
None.

Syntax
Directory string

Maximum Length
128

Value Single-valued

ibm-slapdKrbAdminDN

Description
Specifies the Kerberos ID of the LDAP administrator (for example, ibm-kn=admin1@realm1). Used when Kerberos authentication is used to authenticate the administrator when logged onto the Server Administration interface. This attribute might be specified instead of or in addition to adminDN and adminPW.

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
128

Value Single-valued

ibm-slapdKrbEnable

Description
Specifies whether the server supports Kerberos authentication. It must be either TRUE or FALSE.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdKrbIdentityMap

Description
Specifies whether to use Kerberos identity mapping. It must be set to either TRUE or FALSE. If set to TRUE, when a client is authenticated with a Kerberos ID, the server searches for all local users with matching Kerberos credentials, and adds those user DNs to the bind credentials of the connection. This allows ACLs based on LDAP user DNs to still be usable with Kerberos authentication.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdKrbKeyTab

Description
Specifies the LDAP server Kerberos keytab file. This file contains the LDAP server private key, that is associated with its Kerberos account. This file is to be protected (like the server SSL key database file).

On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and any path not preceded by a drive letter. (D:) is assumed to be rooted at the installation directory (that is: /tmp/slapd.errors = D:\Program Files\IBM\ldap\tmp\slapd.errors).

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdKrbRealm

Description
Specifies the Kerberos realm of the LDAP server. It is used to publish the ldapservicename attribute in the root DSE. Note that an LDAP server can serve as the repository of account information for multiple KDCs (and realms), but the LDAP server, as a server that is using Kerberos, can only be a member of a single realm.

Default
No preset default is defined.

Syntax
Directory string with case-insensitive matching

Maximum Length
256

Value Single-valued

ibm-slapdLanguageTagsEnabled

Description
Whether or not the server should allow language tags. The value read from the ibmslapd.conf file for this attribute is FALSE, but, can be set to TRUE.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdLdapCrlHost

Description
Specifies the host name of the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter is needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation.

Default
No preset default is defined.

Syntax
Directory string with case-insensitive matching

Maximum Length
256

Value Single-valued

ibm-slapdLdapCrlPassword

Description
Specifies the password that server-side SSL uses to bind to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter might be needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation.

Note: If the LDAP server holding the CRLs permits unauthenticated access to the CRLs (that is, anonymous access), then ibm-slapdLdapCrlPassword is not required.

Default
No preset default is defined.

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdLdapCrlPort

Description
Specifies the port used to connect to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter is needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation. (IP ports are unsigned, 16-bit integers in the range 1 - 65535)

Default
No preset default is defined.

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdLdapCrlUser

Description
Specifies the bindDN that the server-side SSL uses to bind to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter might be needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation.

Note: If the LDAP server holding the CRLs permits unauthenticated access to the CRLs (that is, anonymous access), then ibm-slapdLdapCrlUser is not required.

Default
No preset default is defined.

Syntax
DN

Maximum Length
1000

Value Single-valued

ibm-slapdMasterDN

Description
Specifies the bind DN of master server. The value must match the replicaBindDN in the replicaObject defined for the master server. When Kerberos is used to authenticate to the replica, ibm-slapdMasterDN must

specify the DN representation of the Kerberos ID (for example, ibm-kn=freddy@realm1). When Kerberos is used, MasterServerPW is ignored.

Default
No preset default is defined.

Syntax
DN

Maximum Length
1000

Value Single-valued

ibm-slapdMasterPW

Description
Specifies the bind password of master replica server. The value must match replicaBindDN in the replicaObject defined for the master server. When Kerberos is used to authenticate to the replica, ibm-slapdMasterDN must specify the DN representation of the Kerberos ID (for example, ibm-kn=freddy@realm1). When Kerberos is used, MasterServerPW is ignored.

Default
No preset default is defined.

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdMasterReferral

Description
Specifies the URL of the master replica server. For example:

```
ldap://master.us.ibm.com
```

For security set to SSL only:

```
 ldaps://master.us.ibm.com:636
```

For security set to none and use a nonstandard port:

```
ldap://master.us.ibm.com:1389
```

Default
none

Syntax
Directory string with case-insensitive matching

Maximum Length
256

Value Single-valued

ibm-slapdMaxEventsPerConnection

Description
Specifies the maximum number of event notifications that can be registered per connection.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
100

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxEventsTotal

Description
Specifies the maximum total number of event notifications that can be registered for all connections.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
0

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxNumOfTransactions

Description
Specifies the maximum number of transactions per server.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
20

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxOpPerTransaction

Description
Specifies the maximum number of operations per transaction.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
5

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxPendingChangesDisplayed

Description
Maximum number of pending changes to be displayed.

Default
200

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxTimeLimitOfTransactions

Description
Specifies the maximum timeout value of a pending transaction in seconds.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
300

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdPagedResAllowNonAdmin

Description
Whether or not the server should allow non-administrator bind for paged results requests on a search request. If the value read from the ibmslapd.conf file is FALSE, the server will process only those client requests submitted by a user with administrator authority. If a client requests paged results for a search operation, does not have administrator authority, and the value read from the ibmslapd.conf file for this attribute is FALSE, the server will return to the client with return code insufficientAccessRights; no searching or paging will be performed.

Default
FALSE

Syntax
Boolean

Length
5

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Objectclass
ibm-slapdRdbmBackend

Required
No

ibm-slapdPagedResLmt

Description
Maximum number of outstanding paged results search requests allowed active simultaneously. Range = 0.... If a client requests a paged results operation, and a maximum number of outstanding paged results are currently active, then the server will return to the client with return code of busy; no searching or paging will be performed.

Default
3

Syntax
Integer

Length
11

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Required
No

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Description
Maximum number of entries to return from a search for an individual page when paged results control is specified, regardless of any pagesize that might have been specified on the client search request. Range = 0.... If a client has passed a page size, then the smaller value of the client value and the value read from ibmslapd.conf will be used.

Default
50

Syntax
Integer

Length
11

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Required
No

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Description
A plug-in is a dynamically loaded library that extends the capabilities of the server. An ibm-slapdPlugin attribute specifies to the server how to load and initialize a plug-in library. The syntax is:

`*keyword filename* init_function [*args*...]`

The syntax is slightly different for each platform because of library naming conventions. See the *Server Plug-ins Reference* for a list of plug-ins included with IBM Tivoli Directory Server.

Most plug-ins are optional, but the RDBM backend plug-in is required for all RDBM backends.

Default
database /bin/libback-rdbm.dll rdbm_backend_init

Syntax
Directory string with case-exact matching

Maximum Length
2000

Value Multi-valued

ibm-slapdPort

Description
Specifies the TCP/IP port used for non-SSL connections. It cannot have the same value as ibm-slapdSecurePort. (IP ports are unsigned, 16-bit integers in the range 1 - 65535.)

Default
389

Syntax
Integer

Maximum Length
5

Value Single-valued

ibm-slapdPWEncryption

Description
Specifies the encoding mechanism for the user passwords before they are stored in the directory. It must be specified as none, imask, crypt, or sha (you must use the keyword **sha** in order to get SHA-1 encoding). The value must be set to none for the SASL cram-md5 bind to succeed.

Default
none

Syntax
Directory string with case-insensitive matching

Maximum Length
5

Value Single-valued

ibm-slapdReadOnly

Description
This attribute is normally applied to only the Directory backend. It specifies whether the backend can be written to. It must be specified as either TRUE or FALSE. It defaults to FALSE if unspecified. If set to TRUE, the server returns LDAP_UNWILLING_TO_PERFORM (0x35) in response to any client request that changes data in the readOnly database.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdReferral

Description
Specifies the referral LDAP URL to pass back when the local suffixes do not match the request. It is used for superior referral (that is, the suffix is not within the naming context of the server).

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
32700

Value Multi-valued

ibm-slapdReplDbConns

Description
Maximum number of database connections for use by replication.

Default
4

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdReplicaSubtree

Description
Identifies the DN of a replicated subtree

Syntax
DN

Maximum Length
1000

Value Single-valued

ibm-slapdSchemaAdditions

Description
The ibm-slapdSchemaAdditions attribute is used to identify explicitly which file holds new schema entries. This attribute is set by default to be /etc/V3.modifiedschema. If this attribute is not defined, the server reverts to using the last ibm-slapdIncludeSchema file as in previous releases.

Before Version 3.2, the last includeSchema entry in **slapd.conf** was the file to which any new schema entries were added by the server if it received an add request from a client. Normally the last includeSchema is the V3.modifiedschema file, which is an empty file installed just for this purpose.

Note: The name modified is misleading, for it only stores new entries. Changes to existing schema entries are made in their original files.

Default
/etc/V3.modifiedschema

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdSchemaCheck

Description
Specifies the schema checking mechanism for the add/modify/delete operation. It must be specified as V2, V3, or V3_lenient.

- V2 - Retain v2 and v2.1 checking. Recommended for migration purpose.
- V3 - Perform v3 checking.
- V3_lenient - Not all parent object classes are needed. Only the immediate object class is needed when adding entries.

Default
V3_lenient

Syntax
Directory string with case-insensitive matching

Maximum Length
10

Value Single-valued

ibm-slapdSecurePort

Description
Specifies the TCP/IP port used for SSL connections. It cannot have the same value as ibm-slapdPort. (IP ports are unsigned, 16-bit integers in the range 1 - 65535.)

Default
636

Syntax
Integer

Maximum Length
5

Value Single-valued

ibm-slapdSecurity

Description
Enables SSL connections. Must be none, SSL, or SSLOnly.

- none - server listens on the non-ssl port only.
- SSL - server listens on both the ssl and the non-ssl ports.
- SSLOnly - server listens on the ssl port only.

Default
none

Syntax
Directory string with case-insensitive matching

Maximum Length
7

Value Single-valued

ibm-slapdServerId

Description
Identifies the server for use in replication.

Syntax
IA5 String with case-sensitive matching

Maximum Length
240

Value Single-valued

ibm-slapdSetenv

Description
The server runs **putenv()** for all values of ibm-slapdSetenv at startup to modify the server runtime environment. Shell variables (like %PATH% or $LANG) are not expanded.

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
2000

Value Multi-valued

ibm-slapdSizeLimit

Description
The maximum number of entries to return from search, regardless of any size limit that might have been specified on the client search request (Range = 0...). If a client has passed a limit, then the smaller value of the client values and the value read from the ibmslapd.conf file are used. If a client has not passed a limit and has bound as admin DN, the limit is considered unlimited. If the client has not passed a limit and has not bound as admin DN, then the limit is that which was read from the ibmslapd.conf file. 0 = unlimited.

Default
500

Syntax
Integer

Maximum Length
12

Value Single-valued

ibm-slapdSortKeyLimit

Description
The maximum number of sort conditions (keys) that can be specified on a single search request. Range = 0.... If a client has passed a search request with more sort keys than the limit allows, and the sorted search control criticality is FALSE, then the server will honor the value read from the ibmslapd.conf file and ignore any sort keys encountered after the limit has been reached - searching and sorting will be performed. If a client has passed a search a request with more keys than the limit allows, and the sorted search control criticality is TRUE, then the server will return to the client with a return code of **adminLimitExceeded** - no searching or sorting will be performed.

Default
3

Syntax
cis

Length
11

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Objectclass
ibm-slapdRdbmBackend

Required
No

ibm-slapdSortSrchAllowNonAdmin

Description
Whether or not the server should allow non-administrator bind for sort on a search request. If the value read from the ibmslapd.conf file is FALSE, the server will process only those client requests submitted by a user with administrator authority. If a client requests sort for a search operation, does not have administrator authority, and the value read from the ibmslapd.conf file for this attribute is FALSE, the server will return to the client with return code insufficientAccessRights - no searching or sorting will be performed.

Default
FALSE

Syntax
Boolean

Length
5

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Objectclass
ibm-slapdRdbmBackend

Required
No

ibm-slapdSslAuth

Description
Specifies the authentication type for the SSL connection, either serverauth or serverclientauth.

- serverauth - supports server authentication at the client. This is the default.

- serverclientauth - supports both server and client authentication.

Default
serverauth

Syntax
Directory string with case-insensitive matching

Maximum Length
16

Value Single-valued

ibm-slapdSslCertificate

Description
Specifies the label that identifies the server Personal Certificate in the key database file. This label is specified when the server private key and certificate are created with the **gsk4ikm** application. If ibm-slapdSslCertificate is not defined, the default private key, as defined in the key database file, is used by the LDAP server for SSL connections.

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
128

Value Single-valued

ibm-slapdSslCipherSpec

Specifies the method of SSL encryption for clients accessing the server. Must be set to one of the following:

Table 5. Methods of SSL encryption

Attribute	Encryption level
TripleDES-168	Triple DES encryption with a 168-bit key and a SHA-1 MAC
DES-56	DES encryption with a 56-bit key and a SHA-1 MAC
RC4-128-SHA	RC4 encryption with a 128-bit key and a SHA-1 MAC
RC4-128-MD5	RC4 encryption with a 128-bit key and a MD5 MAC
RC2-40-MD5	RC4 encryption with a 40-bit key and a MD5 MAC
RC4-40-MD5	RC4 encryption with a 40-bit key and a MD5 MAC
AES	AES encryption

Syntax
IA5 String

Maximum Length
30

ibm-slapdSslFIPsModeEnabled

Description
If TRUE, specifies that the server will use the ICC version of GSKit ; if FALSE, specifies that the server will use the BSAFE version.

Default
Varies by platform

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdSslKeyDatabase

Description
Specifies the file path to the LDAP server SSL key database file. This key database file is used for handling SSL connections from LDAP clients, as well as for creating secure SSL connections to replica LDAP servers.

On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and a leading slash not preceded by a drive specifier (D:) is assumed to be rooted at the installation directory (that is, /etc/key.kdb = D:\Program Files\IBM\ldap\etc\key.kdb).

Default
/etc/key.kdb

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdSslKeyDatabasePW

Description
Specifies the password associated with the LDAP server SSL key database file, as specified on the ibm-slapdSslKeyDatabase parameter. If the LDAP server key database file has an associated password stash file, then the ibm-slapdSslKeyDatabasePW parameter can be omitted, or set to none.

Note: The password stash file must be located in the same directory as the key database file and it must have the same file name as the key database file, but with an extension of .sth instead of .kdb.

Default
none

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdSslKeyRingFile

Description
Path to the LDAP server's SSL key database file. This key database file is used for handling SSL connections from LDAP clients, as well as for creating secure SSL connections to replica LDAP servers. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive specifier is assumed to be rooted at the installation directory (for example, /etc/key.kdb = c:\Program Files\IBM\ldap\etc\key.kdb).

Default
key.kdb

Syntax
Directory String with case-sensitive matching

Maximum Length
1024

Value Single-valued

ibm-slapdStartupTraceEnabled

Description
Specifies whether trace information is to be collected at server startup. Must be TRUE or FALSE.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdSuffix

Description
Specifies a naming context to be stored in this backend.

Note: This has the same name as the object class.

Default
No preset default is defined.

Syntax
DN

Maximum Length
1000

Value Multi-valued

ibm-slapdSupportedWebAdmVersion

Description
This attribute defines the earliest version of the Web Administration Tool that supports this server of cn=configuration.

Default

Syntax
Directory String

Maximum Length

Value Single-valued

ibm-slapdSysLogLevel

Description
Specifies the level at which debugging and operation statistics are logged in the slapd.errors file. It must be specified as l, m, or h.

- h - high (provides the most information)
- m - medium (the default)
- l - low (provides the least information)

Default
m

Syntax
Directory string with case-insensitive matching

Maximum Length
1

Value Single-valued

ibm-slapdTimeLimit

Description
Specifies the maximum number of seconds to spend on a search request, regardless of any time limit that might have been specified on the client request. If a client has passed a limit, then the smaller value of the client values and the value read from **ibmslapd.conf** are used. If a client has not passed a limit and has bound as admin DN, the limit is considered unlimited. If the client has not passed a limit and has not bound as admin DN, then the limit is that which was read from the **ibmslapd.conf** file. 0 = unlimited.

Default
900

Syntax
Integer

Maximum Length

Value Single-valued

ibm-slapdTraceMessageLevel

Description
Sets the debug message level. Use the command `ibmslapd -h ?` to see the available levels.

Default
0xFFFF (or 65535)

Syntax
Directory string

Maximum Length
16

Value Single-valued

ibm-slapdTraceMessageLog

Description
File path or device on the ibmslapd host computer to which LDAP C API and Debug macro messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the installation directory (for example, /tmp/tracemsg.log = C:\Program Files\IBM\ldap\tmp\tracemsg.log).

Default
Varies by platform

Syntax
Directory string

Maximum Length
1024

Value Single-valued

ibm-slapdTransactionEnable

Description
If the transaction plug-in is loaded but ibm-slapdTransactionEnable is set to FALSE, the server rejects all StartTransaction requests with the response `LDAP_UNWILLING_TO_PERFORM`.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdUseProcessIdPw

Description
If set to TRUE, the server ignores the ibm-slapdDbUserID and the ibm-slapdDbUserPW attributes and uses its own process credentials to authenticate to DB2.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdVersion

Description
IBM Slapd version Number

Default

Syntax
Directory String with case-sensitive matching

Maximum Length

Value Single-valued

ibm-slapdWriteTimeout

Description
Specifies a timeout value in seconds for blocked writes. When the time limit is reached the connection will be dropped.

Default
120

Syntax
Integer

Maximum Length
1024

Value Single-valued

objectClass

Description
The values of the objectClass attribute describe the kind of object that an entry represents.

Syntax
Directory string

Maximum Length
128

Value Multi-valued

Appendix L. Notices

This information was developed for products and services offered in the U.S.A. IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 1998, 2003

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department MU5A46
11301 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AIX
DB2
IBM
iSeries
OS/400
pSeries
RS/6000
S/390
SecureWay

SP
Tivoli
WebSphere
xSeries
z/OS
zSeries

Intel, Intel Inside (logos), MMX™ and Pentium® are trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Index

A

- administrator DN and password, setting
  - Configuration Tool 84
  - ldapcfg 93
- AdminTool 68
- AIX
  - command line 60
  - SMIT 58
- AIX client system requirements 13
- AIX server system requirements 19
- application server, starting 97

B

- backing up database
  - Configuration Tool 92
  - dbback 96

C

- change log, disabling
  - Configuration Tool 88
  - ldapucfg 99
- change log, enabling
  - Configuration Tool 88
  - ldapcfg 95
- character set
  - IANA 136
- client
  - removing 100
  - system requirements 13
- code page, DB2 136
- configuration 143
  - after installation 83
  - embedded version of WebSphere Application Server - Express 125
  - environments
    - HP-UX 76
  - ldapcfg 92
  - ldapxcfg 83
  - overview 10, 83
  - planning
    - database 119
  - troubleshooting 107
- Configuration Tool 83
- configuring database
  - Configuration Tool 86
  - ldapcfg 93

D

- database
  - configuration planning 119
    - access permissions 119
    - code page 119
    - security requirements 119
    - structure 119
    - type of data 119
  - performance 110
- database configuration
  - troubleshooting 109
- database instance 86, 93
- database owner
  - creating 85
  - requirements 85
- database owner on Windows
  - creating 50
  - requirements 50
- database, backing up
  - Configuration Tool 92
  - dbback 96
- database, configuring
  - Configuration Tool 86
  - ldapcfg 93
- database, optimizing
  - Configuration Tool 92
  - runstats 96
- database, restoring
  - Configuration Tool 92
  - dbrestore 96
- database, unconfiguring
  - Configuration Tool 87
  - ldapucfg utility 99
- DB2
  - code page 136
  - performance 110
  - version supplied 3
- DB2 administrator password, changing
  - ldapcfg 95
- debugging 111
- Directory Services Markup Language
  - configuring 131
  - documentation 131
  - installing 131
- DSML
  - configuring 131
  - documentation 131
  - installing 131

E

- embedded version of WebSphere Application Server - Express
  - configuration 125
  - installation 125
  - starting 97
  - uninstalling 125
  - upgrading 43
  - version supplied 3
- enhancements, product 3
- exporting LDIF data
  - Configuration Tool 91
  - db2ldif 95

G

- GSKit 28
  - installing 65
    - AIX 61
    - HP-UX 75
    - Linux 65
    - Solaris 71
    - Windows 80
  - removing
    - AIX 62
    - HP-UX 76
    - Linux 65
    - Solaris 72
    - Windows 81
  - setting up for CMS key databases 139
  - version supplied 3

H

- HP-UX
  - before installing 73
  - setting kernel configuration parameters 73
  - setting system variables 76
- HP-UX client system requirements 17
- HP-UX server system requirements 25

I

- IANA 136
- ibmslapd command 97
- importing LDIF data
  - Configuration Tool 90
  - ldif2db 95
- installation
  - AdminTool 68
  - AIX utilities 57
  - embedded version of WebSphere Application Server - Express 125
  - HP-UX 75
  - installp 60
  - InstallShield GUI 49
    - UNIX 53, 54
    - Windows 50
  - InstallShield GUI on Windows
    - before installing 49
  - Linux 63
  - logs 105
  - manual
    - AIX 57
    - HP-UX 73
    - Linux 63
    - Solaris 67
    - Windows NT 77
  - overview 10
  - pkgadd 69
  - silent 77
  - SMIT 58
  - Solaris 67
  - Solaris command line 69
  - troubleshooting 105

© Copyright IBM Corp. 1998, 2003

InstallShield GUI
  before installing 49
  overview 49
instance name 86, 93
iSeries Linux client system requirements 16
iSeries Linux server
  system requirements 23
iso file, IBM Tivoli Directory Server 9

K

kernel configuration parameters
  HP-UX 73

L

LDAP, other vendors 9
ldapcfg 92
ldapucfg 99
ldapxcfg 83
LDIF data, exporting
  Configuration Tool 91
  db2ldif 95
LDIF data, importing
  Configuration Tool 90
  ldif2db 95
LDIF data, validating 91
loading sample database 133
locale 136
logs, installation 105

M

Microsoft Internet Explorer 28
migration
  database 38, 39
  from IBM Directory Server 4.1 or 5.1
    AIX installations 37
    UNIX installations 42
    Windows installations 37
  from SecureWay Directory
    AIX installations 33
    UNIX installations 35
    Windows InstallShield GUI installations 30
  overview 9, 29
  replica servers 123
  troubleshooting 116
  Web Administration Tool 43
Mozilla 28

N

national language characters 135
new function in IBM Tivoli Directory Server 5.2 3

O

optimizing database
  Configuration Tool 92
  runstats 96

P

package dependencies, Solaris 67
pkgadd 69
prerequisites
  client 13
  server 18
pSeries Linux client system requirements 16
pSeries Linux server
  system requirements 23

R

removing
  client 100
  IBM Tivoli Directory Server
    AIX 101
    HP-UX 102
    InstallShield GUI 100
    Linux 101
    Solaris 101
    UNIX platforms 100
    Windows 100
  server 100
replica servers, migrating 123
restoring database
  Configuration Tool 92
  dbrestore 96
RS/6000 SP environment, installation on node 58

S

sample database, loading 133
schema file, adding 89
schema file, changing validation type 90
schema file, removing 89
schema, configuration
  configuration 143
security
  GSKit 28
  SSL 28
server
  removing 100
  starting 97
  system requirements 18
server utilities
  bulkload 135
  db2ldif 135
  ldif2db 135
servers
  types administered by Web Administration Tool 26
setting system variables
  AIX 62
  HP-UX 76
silent installation
  options file 79
  overview 77
  using 77
  verifying 78
SMIT installation 58
Solaris
  AdminTool 68
  command line 69
  Non-IBM version of LDAP 55, 68
Solaris client system requirements 16
Solaris server
  system requirements 24
SSL 28
starting Web Administration Tool 97
suffix, adding
  Configuration Tool 88
  ldapcfg 95
suffix, removing 89
system requirements
  AIX client 13
  AIX server 19
  client 13
  HP-UX client 17
  HP-UX server 25
  iSeries Linux client 16
  iSeries Linux server 23
  pSeries Linux client 16
  pSeries Linux server 23
  server 18
  Solaris client 16
  Solaris server 24
  Web Administration Tool 26
  Windows client 13
  Windows server 18
  xSeries Linux client 14
  xSeries Linux server 21
  zSeries Linux client 15
  zSeries Linux server 22
system variables, setting
  AIX 62
  HP-UX 76

T

tar file, IBM Tivoli Directory Server 9
troubleshooting 105
  configuration 107
  debugging 111
  installation 105
  migration 116
  Web browser 117

U

unconfiguring
  database 87, 99
uninstalling
  client 100
  embedded version of WebSphere Application Server - Express 126
  server 100
UTF-8 135
utilities, server
  bulkload 135
  db2ldif 135
  ldif2db 135

V

validating LDIF data 91

W

Web Administration Tool
  starting 97
  system requirements 26
  types of servers administered by 26
Web browser
  Microsoft Internet Explorer 28
  Mozilla 28
  troubleshooting 117
Windows client system requirements 13
Windows server
  system requirements 18

X

xSeries Linux client system requirements 14
xSeries Linux server
  system requirements 21

Z

zip file, IBM Tivoli Directory Server 9
zSeries Linux client system requirements 15
zSeries Linux server
  system requirements 22

Printed in U.S.A.

SC32-1338-00